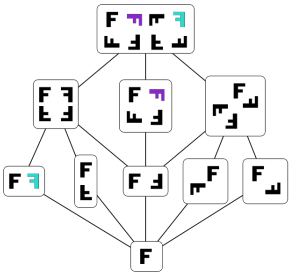
TRABAJO DE FIN DE GRADO

GRADO EN MATEMÁTICAS

*Rubén Tellechea Zamanillo*



# Resultados sobre determinación de grupos por su orden y el de sus elementos


UNIVERSIDAD
COMPLUTENSE
MADRID

*Bajo la dirección de José Javier Etayo Gordejuela*

FACULTAD DE CIENCIAS MATEMÁTICAS

DEPARTAMENTO DE ÁLGEBRA, GEOMETRÍA Y TOPOLOGÍA

Curso 2018 – 2019

*(En orden cronológico)*
*A Mamá y Papá.*

## Abstract

In this work we determine possible groups which a group can be isomorphic to, once its order has been fixed or one of its elements specified, using elementary methods of group theory in the management of three tools: semidirect products, group extensions and automorphism groups of some of the best known families.

In the first three chapters we will expose these tools, and in the following ones we determine all groups of order $p$, $p^2$, $p^3$, $2p$, $4p$, $pq$ and $2k$ when the group has an element of order $k$.



## Resumen

En este trabajo determinamos los posibles grupos a los que un grupo puede ser isomorfo una vez se ha fijado su orden o especificado el de alguno de sus elementos, haciendo uso de métodos elementales de teoría de grupos en el manejo de tres herramientas: el producto semidirecto, las extensiones de grupos y los grupos de automorfismos de algunas de las familias más conocidas.

En los primeros tres capítulos expondremos dichas herramientas, y en los siguientes determinamos los grupos de orden $p$, $p^2$, $p^3$, $2p$, $4p$, $pq$ y $2k$ cuando el grupo tiene un elemento de orden $k$.

# Índice general

# Glosario de símbolos

| | |
|---|---|
| $G$ | Grupo |
| $H, K$ | Subgrupos |
| $N$ | Subgrupo normal |
| $g, h, k, n, x, y, z$ | Elementos |
| $[g, h]$ | Conmutador de $g$ y $h$, $[g, h] = ghg^{-1}h^{-1}$ |
| $[H, K]$ | Subgrupo de conmutadores, $\{[h, k] \in G : h \in H, k \in K\}$ |
| $\langle g_1, ..., g_n \rangle$ | Subgrupo generado por los elementos $g_1, ..., g_n$ |
| $f, \phi, \varphi$ | Homomorfismos |
| $ker(f)$ | Núcleo del homomorfismo, $\{g \in G : f(g) = 1\}$ |
| $Im(f)$ | Imagen del homomorfismo, $f(G)$ |
| $G \cong H$ | $G$ es isomorfo a $H$, $\exists f : G \to H$ homomorfismo y biyectiva. |
| $o(G)$ | Orden de $G$ |
| $o(g)$ | Orden de $g$ |
| $[G : H]$ | Índice de $H$ sobre $G$, $o(G)/o(H)$ |
| $G/N$ | Grupo cociente de $G$ sobre $N$ |
| $Z(G)$ | Centro del grupo, $\{g \in G : gh = hg, \forall h \in G\}$ |
| $\mathrm{N}_G(H)$ | Normalizador de $H$ en $G$, $\{g \in G : gHg^{-1} = H\}$ |
| $Aut(G)$ | Grupo de automorfismos de $G$, $\{f : G \to G : f$ homomorfismo y biyectiva $\}$ |
| $G \times H$ | Producto directo de $G$ y $H$ |
| $C_n$ | Grupo cíclico de orden $n$, $\langle g \mid g^n = 1 \rangle$ |
| $D_n$ | Grupo dihedral de orden $2n$, $\langle g, h \mid g^n = h^2 = 1, hgh^{-1} = g^{-1} \rangle$ |
| $DC_n$ | Grupo dicíclico de orden $4n$, $\langle g, h \mid g^{2n} = h^4 = 1, g^n = h^2, hgh^{-1} = g^{-1} \rangle$ |
| $Q = DC_2$ | Grupo cuaternión, $\langle i, j \mid i^4 = j^4 = 1, jij^{-1} = i^{-1} \rangle$ |
| $QA_n$ | Grupo quasiabeliano de orden $2^{n+1}$, $\langle g, h \mid g^{2^n} = h^2 = 1, hgh^{-1} = g^{1+2^{n-1}} \rangle$ |
| $QD_n$ | Grupo semidihedral de orden $2^{n+1}$, $\langle g, h \mid g^{2^n} = h^2 = 1, hgh^{-1} = g^{-1+2^{n-1}} \rangle$ |
| $\mathbb{N}$ | Conjunto de números naturales |
| $n, m, a, b$ | Números naturales |
| $\mathbb{P}$ | Conjunto de números naturales primos |
| $p, q$ | Números primos |
| $mcm(a, b)$ | Mínimo común múltiplo de $a$ y $b$. |
| $mcd(a, b)$ | Máximo común divisor de $a$ y $b$. |
| $a \mid b$ | $a$ es divisor de $b$, $\exists m \in \mathbb{N} : am = b$ |
| $a \equiv b(c)$ | $a$ es congruente con $b$ módulo $c$, $\exists m \in \mathbb{N} : cm = a - b$ |

# Introducción

> — [...] De otra suerte, la cosa más poética del mundo sería nuestro tranvía subterráneo.
> — Y así es, en efecto. [...] Lo raro y hermoso es tocar la meta; lo fácil y vulgar es fallar. Nos parece cosa de epopeya que el flechero alcance desde lejos a un ave con un dardo salvaje, ¿y no debería parecérnoslo que el hombre le acierte desde lejos a una estación con una máquina salvaje? El caos es imbécil, por lo mismo que allí el tren puede ir igualmente a Baker Street o a Bagdad. Pero el hombre es un verdadero mago, y toda su magia consiste en que dice el hombre: «¡sea Victoria!», y hela que aparece.
>
> G.K. Chesterton, *El hombre que fue jueves.*

El de la clasificación de todos los grupos finitos (dar una lista de éstos tal que cualquier grupo finito sea isomorfo a uno de la lista, pero ningunos dos de la lista sean isomorfos entre sí) es un problema que viene de lejos. Formas más modestas de esta cuestión han sido resueltas en los últimos años: tenemos tales listas para los grupos finitos abelianos [9], para los grupos finitos simples [1], para todos los grupos de orden menor que 2000 (salvo orden 1024) [2] ... y sin embargo su planteamiento general se mantiene irresoluto. A lo largo de estas páginas abordaremos una parte ínfima de dicho problema: daremos listas como la descrita arriba para los grupos que tengan un determinado orden que hayamos fijado, y trataremos que ese orden sea tan genérico y abarque tantos casos como sea posible. Más bien nos conformaremos con dar una familia de grupos a la que cualquiera en tales circunstancias sea isomorfo a uno de ellos, y dejaremos al lector que compruebe que ningunos dos son isomorfos entre sí, ya que la resolución llenaría páginas apelando a una cuestión sin mucho interés ni dificultad; basta echar un vistazo a los resultados y jugar un poco con las cuentas para darse cuenta de que en efecto es así.

El primer punto que debemos tratar es el producto semidirecto, herramienta imprescindible en la tarea de buscar grupos por la manera en que éste simplifica muchos de ellos. No obstante, cuando uno tiene un martillo piensa que todos los problemas son clavos, y en este caso la cosa no es así. Para ello, el segundo capítulo señalará (viéndolo desde una perspectiva más amplia) las limitaciones que tiene dicho producto, quedando advertidos sobre posibles errores en su uso. Terminaremos el repertorio técnico viendo los grupos de automorfismos que vamos a requerir. Con todo ello, daremos las listas de los grupos de órdenes $p$, $p^2$, $p^3$, $2p$, $4p$, y $pq$. Cerraremos el trabajo con un problema de ámbito más concreto, pero igualmente encauzado en el hilo que llevamos.

Huelga decir que todo lo que no se define aquí requiere tan sólo de métodos elementales, que se aprenden en cualquier curso de teoría de grupos, y por consiguiente a cualquier alumno que haya cursado uno no le debería presentar mayor dificultad. Para aliviar algunas lagunas leves en la memoria hemos decidido incluir junto a la notación las definiciones de los términos que se presuponen, y para olvidos mayores recomendamos acudir a [4].

# Capítulo 1

# Producto semidirecto

El producto semidirecto va a ser la herramienta fundamental en la labor de clasificar grupos, pues gracias a ella nos basta con localizar dos subgrupos «complementarios», con uno de ellos normal, para tener finalizada la clasificación.

En lo que sigue, llamaremos de manera informal «complementarios» a una pareja de subgrupos tales que su intersección es el subgrupo trivial y su producto el grupo total.

## 1.1. Introducción y definiciones

Esta primera proposición nos muestra la relación entre la estructura de estos subgrupos «complementarios» y la del grupo original cuando uno de ellos es normal, mostrando que en su producto cartesiano como conjuntos podemos definir una operación que se corresponde con la del grupo que los contiene.

**Proposición 1.1.1.** *Sea $G$ un grupo y sean $N, H < G$ subgrupos suyos, con $N \triangleleft G$, $NH = G$, $N \cap H = \{1_G\}$. Dotemos al conjunto $N \times H$ con la operación*

$$\begin{aligned} \circ : (N \times H) \times (N \times H) &\longrightarrow N \times H \\ (n_1, h_1), (n_2, h_2) &\longmapsto (n_1 h_1 n_2 h_1^{-1}, h_1 h_2) \end{aligned}$$

*Entonces $(N \times H, \circ)$ es grupo y $G \cong (N \times H, \circ)$.*

*Demostración.* Comencemos viendo que $(N \times H, \circ)$ es grupo. Como $N \triangleleft G$, se da $hnh^{-1} \in N, \forall n \in N, \forall h \in H$, de modo que la operación está bien definida y el producto es interno. El elemento neutro es $(1_N, 1_H) \in N \times H$ y dado el elemento $(n, h) \in N \times H$, su inverso es $(h^{-1}n^{-1}h, h^{-1})$. Finalmente, la asociatividad se comprueba tomando $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in N \times H$ y viendo:

$$\begin{aligned} ((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1 h_1 n_2 h_1^{-1}, h_1 h_2)(n_3, h_3) \\ &= ((n_1 h_1 n_2 h_1^{-1}) h_1 h_2 n_3 h_2^{-1} h_1^{-1}, (h_1 h_2) h_3) \\ &= (n_1 h_1 n_2 h_2 n_3 h_2^{-1} h_1^{-1}, h_1 (h_2 h_3)) \\ &= (n_1, h_1)(n_2 h_2 n_3 h_2^{-1}, h_2 h_3) \\ &= (n_1, h_1)((n_2, h_2)(n_3, h_3)) \end{aligned}$$

Veamos ahora la isomorfía buscada. Cada $g \in G$ se puede escribir de forma única de la forma $g = nh, n \in N, h \in H$, ya que, de poderse escribir $n_1 h_1 = n_2 h_2$ con $n_1, n_2 \in N, h_1, h_2 \in H$ tendríamos también $n_2^{-1} n_1 = h_2 h_1^{-1}$, que está claro que pertenece a $N \cap H$, luego es $1_G$, con lo que $n_1 = n_2$ y $h_1 = h_2$.

Tomemos así la función $\gamma : N \times H \to G : (n,h) \mapsto nh$. Es sobreyectiva porque dado $g \in G$ hay unos únicos $n \in N, h \in H$ tales que $g = nh$, y por tanto $\gamma(n,h) = g$. También es inyectiva por la unicidad de la representación $nh$. También es homomorfismo, ya que dados $n_1h_1, n_2h_2 \in G$ tenemos:

$$\begin{aligned}\gamma((n_1,h_1)(n_2,h_2)) &= \gamma((n_1h_1n_2h_1^{-1}, h_1h_2)) = n_1h_1n_2h_1^{-1}h_1h_2 \\ &= n_1h_1n_2h_2 = \gamma(n_1,h_1)\gamma(n_2,h_2)\end{aligned}$$

Q.E.D.

Queda claro, entonces, que la estructura de $G$ queda determinada por la forma en que los elementos de $H$ «mueven internamente» los elementos de $N$. Cada uno de estas movimientos internos $n \mapsto hnh^{-1}$ define, y queda definido, por un automorfismo. Vamos a dar entonces una definición de grupo dependiente de cada posible homomorfismo que enlaza cada elemento $h \in H$ con un automorfismo de $N$, al que llamaremos producto semidirecto por el homomorfismo. Comprobamos, además, que efectivamente la definición que damos determina un grupo.

**Definición 1.1.2.** *Sean $N$ y $H$ grupos y sea $\phi : H \to Aut(N) : h \mapsto \varphi_h$ un homomorfismo. Definimos el producto semidirecto de $N$ y $H$ por $\phi$, denotado por $N \rtimes_\phi H$, al par formado por el conjunto $N \times H$ y la operación*

$$\begin{aligned}\circ : (N \times H) \times (N \times H) &\longrightarrow N \times H \\ (n_1,h_1),(n_2,h_2) &\longmapsto (n_1\phi(h_1)(n_2), h_1h_2)\end{aligned}$$

*Si sólo hay un homomorfismo no trivial lo denotaremos por $N \rtimes H$.*

En general, a ese homomorfismo lo denotaremos siempre por $\phi$ y, dado que $\phi(h)$ es también homomorfismo, por comodidad, lo denotaremos por $\varphi_h$.

**Proposición 1.1.3.** *Sean $N$ y $H$ grupos y sea $\phi : H \to Aut(N)$ un homomorfismo. El producto semidirecto $N \rtimes_\phi H$ es grupo.*

*Demostración.* La operación es claramente interna y está bien definida. El elemento neutro es $(1_N, 1_H) \in N \times H$ y dado el elemento $(n,h) \in N \times H$, su inverso es $(\phi(h^{-1})(n^{-1}), h^{-1})$. Finalmente, la asociatividad se comprueba tomando $(n_1,h_1),(n_2,h_2),(n_3,h_3) \in N \times H$ y viendo:

$$\begin{aligned}((n_1,h_1)(n_2,h_2))(n_3,h_3) &= (n_1\varphi_{h_1}(n_2), h_1h_2)(n_3,h_3) \\ &= ((n_1\varphi_{h_1}(n_2))\varphi_{h_1h_2}(n_3), (h_1h_2)h_3) \\ &= ((n_1\varphi_{h_1}(n_2))\varphi_{h_1}(\varphi_{h_2}(n_3)), (h_1h_2)h_3) \\ &= (n_1\varphi_{h_1}(n_2\varphi_{h_2}(n_3)), h_1(h_2h_3)) \\ &= (n_1,h_1)((n_2,h_2),(n_3,h_3))\end{aligned}$$

Q.E.D.

## 1.2. Producto semidirecto como herramienta de determinación

Con todo lo expuesto queda patente la estrecha relación (de isomorfía) que guarda la operación en un grupo $G$ con la que se ha definido a partir de dos subgrupos «complementarios», $N$ y $H$, cuando uno de ellos es normal: si en un grupo localizamos dos subgrupos con tales propiedades, tendremos perfectamente delimitadas las posibilidades de determinación del grupo, viendo las distintas posibilidades del automorfismo $\phi : H \to Aut(N)$. El siguiente teorema nos orienta en cómo utilizar lo establecido hasta este punto.

**Teorema 1.2.1.** *Sea $G$ un grupo y sean $N, H < G$ subgrupos suyos con $N \triangleleft G$, $NH = G$, $N \cap H = \{1_G\}$. Entonces existe un homomorfismo $\phi : H \to Aut(N)$ tal que $G \cong N \rtimes_\phi H$.*

*Demostración.* Para cada $h \in H$, definamos $\varphi_h : N \to N : n \mapsto hnh^{-1}$, bien definido porque $N \triangleleft G$. Está claro que es automorfismo, pues dados $n_1, n_2 \in N$,

$$\varphi_h(n_1)\varphi_h(n_2) = hn_1h^{-1}hn_2h^{-1} = hn_1n_2h^{-1} = \varphi_h(n_1n_2)$$

Además se cumple que dados $h_1, h_2 \in H$, $\varphi_{h_1} \circ \varphi_{h_2} = \varphi_{h_1h_2}$. En efecto, dado $n \in N$,

$$\varphi_{h_1} \circ \varphi_{h_2}(n) = \varphi_{h_1}(\varphi_{h_2}(n)) = \varphi_{h_1}(h_2nh_2^{-1}) = h_1h_2nh_2^{-1}h_1^{-1} = (h_1h_2)n(h_1h_2)^{-1} = \varphi_{h_1h_2}(n)$$

Tomemos entonces la función

$$\begin{aligned} \phi : H &\longrightarrow Aut(N) \\ h &\longmapsto \varphi_h \end{aligned}$$

También ésta es homomorfismo, pues dados $h_1, h_2 \in H$ se tiene:

$$\phi(h_1h_2) = \varphi_{h_1h_2} = \varphi_{h_1} \circ \varphi_{h_2} = \phi(h_1)\phi(h_2)$$

Con esto queda claro, por 1.1.1, que el homomorfismo $\phi$ define un producto semidirecto que es isomorfo a $G$. Q.E.D.

Ahora bien, cabe la posibilidad de que distintos homomorfismos $\phi : H \to Aut(N)$ determinen productos semidirectos que sean isomorfos entre sí. En otras palabras, en general no hay una correspondencia entre los distintos homomorfismos $\phi : H \to Aut(N)$ y los grupos con dos subgrupos $N$ y $H$ «complementarios» con $N$ normal. Para lidiar con ello, la siguiente proposición nos señala situaciones en las que dos homomorfismos nos generan productos semidirectos isomorfos, lo cual nos ayudará a reducir notablemente la cantidad de homomorfismos a tener en cuenta.

**Proposición 1.2.2.** *Sean $N, H$ dos grupos y $\phi : H \to Aut(N)$ un homomorfismo. Entonces:*

- $\beta \in Aut(H) \Rightarrow N \rtimes_\phi H \cong N \rtimes_{\phi\circ\beta} H$.
- *Sea $\alpha \in Aut(N)$ y sea $\psi : H \to Aut(N) : g \mapsto \alpha\phi(g)\alpha^{-1}$. Entonces $N \rtimes_\phi H \cong N \rtimes_\psi H$*

*Demostración.* Para el primer enunciado consideremos la aplicación $f : N \rtimes_\phi H \to N \rtimes_{\phi\circ\beta} H : (n, h) \mapsto (n, \beta^{-1}(h))$. Claramente es biyectiva y es homomorfismo porque dados $(n_1, h_1), (n_2, h_2) \in N \times H$ se tiene:

$$f((n_1, h_1))f((n_2, h_2)) = (n_1, \beta^{-1}(h_1))(n_2, \beta^{-1}(h_2)) = (n_1\phi(\beta(\beta^{-1}(h_1)(n_2))), \beta^{-1}(h_1)\beta^{-1}(h_2)) =$$
$$(n_1\varphi_{h_1}(n_2), \beta^{-1}(h_1h_2)) = f((n_1\varphi_{h_1}(n_2), h_1h_2)) = f((n_1, h_1)(n_2, h_2))$$

Para el segundo tomemos $f : N \rtimes_\phi H \to N \rtimes_\psi H : (n, h) \mapsto (\alpha(n), h)$. De nuevo, es biyectiva y es homomorfismo. Se comprueba tomando $(n_1, h_1), (n_2, h_2) \in N \times H$ y viendo:

$$\begin{aligned} &f((n_1, h_1))f((n_2, h_2)) = (\alpha(n_1), h_1)(\alpha(n_2), h_2) = (\alpha(n_1)\psi_{h_1}(\alpha(n_2)), h_1h_2) \\ &= (\alpha(n_1)\alpha(\varphi_{h_1}(\alpha^{-1}(\alpha(n_2)))), h_1h_2) = (\alpha(n_1)\alpha(\varphi_{h_1}(n_2)), h_1h_2) = (\alpha(n_1\varphi_{h_1}(n_2)), h_1h_2) \\ &= f(n_1\varphi_{h_1}(n_2), h_1h_2) = f((n_1, h_1)(n_2, h_2)) \end{aligned}$$

Q.E.D.

## 1.3. Producto directo

Llegados a este punto cabría sospechar –aunque sólo fuera por el nombre– que alguna relación guardan el producto semidirecto y el producto directo. Efectivamente, el producto semidirecto es una generalización del producto directo (o, si se quiere, el segundo es un caso particular del primero), ya que basta con tomar el homomorfismo que asocia cada $h \in H$ al automorfismo identidad de $N$ para tener su situación concreta. En este proceso de abstracción, como es natural, se pierden algunas propiedades muy valiosas del producto directo, como que la proyección $\pi_N : N \times H \to N$ sea homomorfismo o que el subgrupo $H < N \times H$ sea normal. A modo de cierre, el siguiente lema deja clara la relación que hay entre dichos conceptos.

**Lema 1.3.1.** *Sean $N, H$ dos grupos y sea $\phi : H \to Aut(N)$ un homomorfismo. Son equivalentes:*

1. $\phi \equiv 1_{Aut(N)}$
2. *La proyección $\pi_N : N \rtimes_\phi H \to N : (n,h) \mapsto n$ es homomorfismo de grupos.*
3. $N \times H \cong N \rtimes_\phi H$*, siendo el isomorfismo la aplicación identidad entre conjuntos.*
4. $\overline{H} \lhd N \rtimes_\phi H$*, siendo* $\overline{H} = \{(1_N, h) \in N \rtimes_\phi H\}$.

*Demostración.* (1) $\Rightarrow$ (2). Dados $(n_1,h_1),(n_2,h_2) \in N \rtimes_\phi H$, tenemos:

$$\pi_N((n_1,h_1)(n_2,h_2)) = \pi_N((n_1\varphi_{h_1}(n_2), h_1h_2)) = n_1\varphi_{h_1}(n_2) = n_1n_2 = \pi_N(n_1,h_1)\pi_N(n_2,h_2)$$

(2) $\Rightarrow$ (3). Es claro que $I : N \rtimes_\phi H \to N \times H : (n,h) \mapsto (n,h)$, la función identidad, es tal que $I = (\pi_N, \pi_H)$. Es claramente biyectiva, y es homomorfismo porque $\pi_N$ lo es por hipótesis y $\pi_H$ lo es por la definición del producto semidirecto.

(3) $\Rightarrow$ (4). Llamemos $\overline{H} = \{(1_N,h) \in N \rtimes_\phi H\}$ al subgrupo del cual queremos probar la normalidad. Dados $(1_N,k) \in \overline{H}, (n,h) \in N \rtimes_\phi H$, tenemos, operando en $N \times H$, pues son isomorfos:

$$(n,h)(1_N,k)(n,h)^{-1} = (n1_Nn^{-1}, hkh^{-1}) = (1_N, hkh^{-1}) \in \overline{H}$$

(4) $\Rightarrow$ (1). Dados $n \in N, h,k \in H$, como $\overline{H} \lhd N \rtimes_\phi H$, se tiene:

$$\begin{aligned}
&(n,h)(1_N,k)(n,h)^{-1} \in \overline{H} \\
&\Rightarrow (n,h)(1_N,k)(\varphi_{h^{-1}}(n^{-1}), h^{-1}) \in \overline{H} \\
&\Rightarrow (n,hk)(\varphi_{h^{-1}}(n^{-1}), h^{-1}) \in \overline{H} \\
&\Rightarrow (n\varphi_{hk}(\varphi_{h^{-1}}(n^{-1})), hkh^{-1}) \in \overline{H} \\
&\Rightarrow (n\varphi_{hkh^{-1}}(n^{-1}), hkh^{-1}) \in \overline{H} \\
&\Rightarrow n\varphi_{hkh^{-1}}(n^{-1}) = 1_N \\
&\Rightarrow \varphi_{hkh^{-1}}(n^{-1}) = n^{-1} && \forall n \in N \\
&\Rightarrow \varphi_{hkh^{-1}} = 1_{Aut(N)} \\
&\Rightarrow \varphi_k = 1_{Aut(N)} && \forall k \in H \\
&\Rightarrow \phi \equiv 1_{Aut(N)}
\end{aligned}$$

Q.E.D.

# Capítulo 2

# Extensiones de grupos

## 2.1. Introducción y definiciones

Planteemos una serie de cuestiones para introducir este capítulo. Tomemos un grupo $N$. Podríamos preguntarnos si hay algún grupo $G$ del que $N$ sea subgrupo normal. La respuesta no es muy complicada: basta tomar $G = N$. En vista de esta facilidad cabría exigir alguna hipótesis más: dado otro grupo $H$, ¿habrá algún grupo $G$ del que $N$ sea subgrupo normal, de modo que además el cociente $G/N$ sea isomorfo a $H$? De nuevo podemos contestar sin esfuerzo: tomando $G = N \times H$ tenemos un subgrupo normal $N \cong \overline{N} = \{(n, 1_H) \in G \times H\} \triangleleft G$, de forma que $G/\overline{N} \cong H$, y esto mismo podríamos decir también para cualquier producto semidirecto. En un caso como este diremos que $G$ es extensión de $N$ por $H$, y lo que podemos preguntarnos finalmente es cuántos grupos $G$ distintos (no isomorfos entre sí) hay que sean extensión de $N$ por $H$, o incluso cuáles son éstos. Para detallar mejor este problema las sucesiones exactas van a ser la herramienta adecuada. Por comodidad, en los siguientes capítulos, en lo que concierne a las sucesiones exactas, denotaremos por 0 al grupo de un único elemento, $\{1\}$.

**Definición 2.1.1.** *Sean $G$, $H$ y $K$ tres grupos y $f : G \to H$ y $g : H \to K$ dos homomorfismos. Diremos que la sucesión*

$$G \xrightarrow{f} H \xrightarrow{g} K$$

*es exacta si $Im(f) = ker(g)$.*

Lo que nos permite dar la definición de extensión.

**Definición 2.1.2.** *Sean $N$ y $H$ dos grupos. Diremos que la terna $(G, i, \pi)$ es una extensión de $N$ por $H$ si $G$ es un grupo e $i : N \to G$ y $\pi : G \to H$ son homomorfismos, de forma que la sucesión*

$$0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$$

*es exacta, es decir, si $i$ es inyectiva, $\pi$ sobreyectiva y $Im(i) = ker(\pi)$. Cuando las aplicaciones $i$ y $\pi$ estén sobreentendidas nos referiremos a $G$ como la extensión de $N$ por $H$, y lo llamaremos grupo extensión en el resto de las situaciones.*

Esto, por supuesto, coincide con lo que hemos dicho hasta ahora. Que $i$ lleve inyectivamente $N$ a $G$ es equivalente a entender $N$ como subgrupo de $G$, ya que $N \cong Im(i) < G$. A su vez, $Im(i) = ker(\pi)$, y sabemos que el núcleo de un homomorfismo es siempre un subgrupo normal, con lo que esta imagen isomorfa a $N$ también lo es. Finalmente, por el primer teorema de isomorfía, $G/ker(\pi) \cong Im(\pi) \cong H$ porque $\pi$ es sobreyectiva, que coincide con lo que pretendíamos, que $G/N \cong H$.

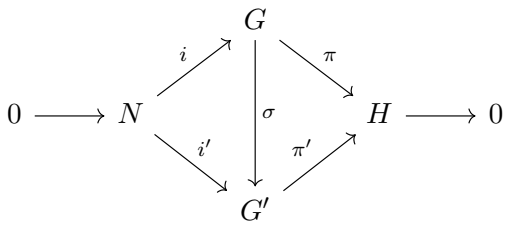
No obstante, en la definición de extensión hemos introducido también las aplicaciones inclusión y proyección sobre el cociente, $i$ y $\pi$, y es importante señalar su importancia, ya que, a veces, algebraicamente, dos extensiones con esas aplicaciones distintas pueden estar cumpliendo el mismo papel. La siguiente definición aclara estas situaciones.

**Definición 2.1.3.** *Dados dos grupos $N$ y $H$, dos extensiones de $N$ por $H$*

$$0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$$

$$0 \longrightarrow N \xrightarrow{i'} G' \xrightarrow{\pi'} H \longrightarrow 0$$

*diremos que son equivalentes cuando exista un isomorfismo $\sigma : G \to G'$ que haga conmutativo el diagrama*




*es decir, que cumpla $\sigma \circ i = i'$ y $\pi' \circ \sigma = \pi$.*

Cabe señalar que, dados dos grupos finitos $N$ y $H$, un grupo extensión $G$ tendrá orden $o(N)o(H)$, y por tanto sólo hay una cantidad finita de posibilidades (no isomorfas entre sí) para $G$. La duda natural ahora es si hay un grupo extensión no isomorfo a los demás por cada extensión no equivalente a las demás. La respuesta es que desgraciadamente no, de forma que las aplicaciones inclusión y proyección sobre el cociente no son un dato superfluo. El siguiente ejemplo no deja lugar a dudas.

**Ejemplo 2.1.4.** Sean $C_9 = \langle a \rangle$ y $C_3 = \langle b \rangle$. Llamemos, en la notación anterior, $N = H = C_3$. Con ello, podemos pensar en las extensiones

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_3 & \xrightarrow{i} & C_9 & \xrightarrow{\pi} & C_3 & \longrightarrow & 0 \\ & & b & \longmapsto & a^3; a & \longmapsto & b & & \end{array}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_3 & \xrightarrow{i'} & C_9 & \xrightarrow{\pi'} & C_3 & \longrightarrow & 0 \\ & & b & \longmapsto & a^6; a & \longmapsto & b & & \end{array}$$

ambas perfectamente definidas. Estas dos no son equivalentes. En efecto, tomemos un isomorfismo $\sigma : C_9 \to C_9$. Si $\sigma \circ i = i'$ tendremos $\sigma(i(b)) = i'(b) = a^6$, luego $\sigma(a^3) = a^6$. Por otro lado, si $\pi' \circ \sigma = \pi$ tendremos $\pi'(\sigma(a)) = \pi(a) = b$; claro que $\pi'^{-1}(\{b\}) \in \{a, a^4, a^7\}$, y si $\sigma(a)$ toma cualquiera de esos valores se dará $\sigma(a^3) = a^3 \neq a^6$. Así, las condiciones $\sigma \circ i = i'$ y $\pi' \circ \sigma = \pi$ son excluyentes, y por tanto las extensiones no equivalentes.

Cualquier extensión con $G = C_3 \times C_3$ no será equivalente a cualquiera de las dos anteriores, ya que los grupos $C_9$ y $C_3 \times C_3$ no son isomorfos. Como veremos en 4.1.2, estos dos son los únicos grupos de orden 9, con lo que hemos encontrado al menos tres extensiones no equivalentes para tan sólo dos grupos no isomorfos.

## 2.2. Producto semidirecto y extensiones

Indagaremos ahora en la relación del producto semidirecto y las extensiones. Dados dos grupos $N$ y $H$ y un homomorfismo $\phi : H \to Aut(N)$ tenemos que $N \cong \overline{N} = \{(n, 1_H) \in N \rtimes_\phi H\} \triangleleft N \rtimes_\phi H$, y que $(N \rtimes_\phi H)/\overline{N} \cong H$. Así, todo producto semidirecto es una extensión

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\ i\ } & N \rtimes_\phi H & \xrightarrow{\ \pi\ } & H & \longrightarrow & 0 \\ & & n & \longmapsto & (n, 1_H); (n, h) & \longmapsto & h & & \end{array}$$

No obstante, no todas las extensiones son productos semidirectos.

**Ejemplo 2.2.1.** Dados los grupos $C_4 = \langle a \rangle$ y $C_2 = \langle b \rangle$, el grupo cuaternión $Q = \langle i, j | i^4 = j^4 = 1_Q, jij^{-1} = i^{-1} \rangle$ es extensión de $C_4$ por $C_2$ con las aplicaciones

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_4 & \longrightarrow & Q & \longrightarrow & C_2 & \longrightarrow & 0 \\ & & a & \longmapsto & i & \longmapsto & 1_{C_2} & & \\ & & & & j & \longmapsto & b & & \end{array}$$

Sin embargo, $Q$ sólo tiene un elemento de orden dos ($i^2 = j^2$), que estará en todo subgrupo isomorfo a $C_4$ (pues este tiene el elemento de orden dos $a^2$) y en todo subgrupo isomorfo a $C_2$ (que también tiene el elemento de orden dos $b$), de modo que es imposible encontrar subgrupos $N$ y $H$ isomorfos a $C_4$ y $C_2$ respectivamente tales que $N \cap H = \{1_Q\}$.

El siguiente teorema nos caracteriza aquellas extensiones de grupos cuyo grupo extendido es producto semidirecto de los grupos que extiende. Para más detalle puede verse en [8].

**Definición 2.2.2.** *Sean los grupos $N$ y $H$ y la extensión $0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$ . Diremos que ésta es separable cuando exista un homomorfismo $\rho : H \to G$ tal que $\pi \circ \rho = Id_H$. A este homomorfismo lo llamaremos corte.*

**Teorema 2.2.3.** *Dados grupos $N$ y $H$, una extensión $0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$ es separable si, y sólo si, $G \cong N \rtimes_\phi H$ para algún homomorfismo $\phi : H \to Aut(N)$.*

*Demostración.* ($\Leftarrow$) Supongamos que tenemos un isomorfismo $f : N \rtimes_\phi H \to G$ para construir la sucesión exacta de la extensión $0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$ y el corte $\rho : H \to G$. Podemos definir los homomorfismos inyectivos $i : N \to G : n \mapsto f(n, 1_H)$ y $\rho : H \to G : h \mapsto f(1_N, h)$. Como $f$ es isomorfismo podemos afirmar que todo elemento en $G$ se corresponde con $f(n, h)$ para algún $(n, h) \in N \rtimes_\phi H$. Definamos así el homomorfismo sobreyectivo $\pi : G \to H : f(n, h) \mapsto h$. Con todo esto es claro que $\pi \circ \rho = Id_H$, pues dado $h \in H$ arbitrario $\pi(\rho(h)) = \pi(f(1_N, h)) = h$; y a su vez

$$Im(i) = \{f(n, 1_H) \in G : n \in N\} = \{f(n, h) \in G : \pi(f(n, h)) = 1_H\} = ker(\pi),$$

que es justo lo que queríamos probar.

($\Rightarrow$) Supongamos ahora una extensión $0 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 0$ y un corte $\rho : H \to G$, y busquemos un homomorfismo $\phi : H \to Aut(N)$ y un isomorfismo $f : G \to N \rtimes_\phi H$. Como $i : N \to Im(i)$ es isomorfismo tomemos su aplicación inversa, $\tau = i^{-1}$, que también es isomorfismo. A su vez, $Im(i) \triangleleft G$ con lo que el elemento $\rho(h)i(n)\rho(h^{-1})$ está en $Im(i)$ para todo $n \in N$ y todo $h \in H$, con lo que dado un $h \in H$ podemos definir la aplicación

$$\begin{array}{c} \varphi_h : N \longrightarrow N \\ n \longmapsto \tau(\rho(h)i(n)\rho(h^{-1})) \end{array}$$

que no es muy difícil comprobar que es automorfismo de $N$. A su vez, con éstos podemos definir la función $\phi : H \to Aut(N) : h \mapsto \varphi_h$, que es homomorfismo porque dado $n \in N$ se da

$$\begin{aligned}(\phi(h_1) \circ \phi(h_2))(n) &= \varphi_{h_1}(\varphi_{h_2}(n)) = \varphi_{h_1}(\tau(\rho(h_2)i(n)\rho(h_2^{-1}))) \\ &= \tau(\rho(h_1)i(\tau(\rho(h_2)i(n)\rho(h_2^{-1})))\rho(h_1^{-1})) \\ &= \tau(\rho(h_1)\rho(h_2)i(n)\rho(h_2^{-1})\rho(h_1^{-1})) \\ &= \tau(\rho(h_1h_2)i(n)\rho((h_1h_2)^{-1})) \\ &= \varphi_{h_1h_2}(n) \\ &= \phi(h_1h_2)(n)\end{aligned}$$

Ahora, si tenemos un elemento $g \in G$, podemos tomar $h_g = \pi(g) \in H$ y $n_g = \tau(g\rho(h^{-1})) \in N$, de forma que $g = i(k)\rho(h)$. De este modo podemos definir la aplicación

$$\begin{aligned} f : G &\longrightarrow N \rtimes_\phi H \\ g &\longmapsto (n_g, h_g)\end{aligned}$$

perfectamente definida por cómo lo están los elementos $n_g$ y $h_g$. Es claro que es una aplicación biyectiva, y necesitamos comprobar que es homomorfismo para tener el resultado buscado. Para esto basta tomar elementos $x, y \in G$ y comprobar que

$$\begin{aligned}f(xy) &= f(i(n_x)\rho(h_x)i(n_y)\rho(h_y)) \\ &= f(i(n_x)\rho(h_x)i(n_y)\rho(h_x^{-1})\rho(h_x)\rho(h_y)) \\ &= f(i(n_x)i(\varphi_{h_x}(n_y))\rho(h_xh_y)) \\ &= f(i(n_x\varphi_{h_x}(n_y))\rho(h_xh_y))) \\ &= (n_x\varphi_{h_x}(n_y), h_xh_y) \\ &= (n_x, h_x)(n_y, h_y) \\ &= f(i(n_x)\rho(h_x))f(i(n_y)\rho(h_y)) \\ &= f(x)f(y)\end{aligned}$$

Q.E.D.

Este último teorema, aunque determina exactamente aquellas situaciones en las que sólo podemos extender utilizando el producto semidirecto, no resulta muy útil para conocer, a partir de datos básicos del grupo extensión $G$ (como por ejemplo su orden, que lo determinan a su vez los órdenes de $N$ y $H$) si dicho producto va a ser la única forma posible de extender. El resultado es valioso, pero sólo nos dice si una extensión es producto semidirecto una vez la tenemos perfectamente (o en gran medida) determinada, lo cual no suele ser el caso.

El resultado siguiente, en cambio, sí que nos va a decir cuando la única forma de extender es el producto semidirecto. La demostración de este teorema, al menos en su comienzo, sólo hace uso de métodos elementales como los que empleamos en este trabajo. Sin embargo, su escollo final requiere de maquinaria más avanzada (bien teoría de representaciones, bien cohomología de grupos) que extendería el trabajo por encima de su límite. Además, ni el teorema ni el lema que necesariamente le precede van a ser usados realmente en el texto (aunque son una buena referencia en el hilo que estamos siguiendo), motivo de más para dejar su prueba en manos de la bibliografía. Puede encontrarse el resultado en [5].

**Lema 2.2.4.** *(Argumento de Frattini) Sea $G$ un grupo y sea $N \lhd G$ un subgrupo normal suyo. Consideremos $P$ un p-subgrupo de Sylow de $N$. Entonces $G = N\mathrm{N}_G(P)$.*

**Teorema 2.2.5.** *(Schur – Zassenhaus) Sea $G$ un grupo finito de orden $ab$, con $a, b \in \mathbb{N}$ y $mcd(a, b) = 1$. Si $G$ tiene un subgrupo normal de orden $a$, entonces tiene un subgrupo de orden $b$.*

El caso concreto siguiente se refiere al problema que hasta ahora hemos estado manejando.

**Corolario 2.2.6.** *Sean $N$ y $H$ dos grupos finitos de órdenes coprimos. Entonces, las extensiones de $N$ por $H$ serán productos semidirectos (aunque no necesariamente de $N$ por $H$).*

*Demostración.* Si $G$ es una extensión de $N$ por $H$, necesariamente tendrá a $N$ como subgrupo normal. Por el teorema 2.2.5 habrá un subgrupo $K < G$ de orden $o(H)$. Como los órdenes de $N$ y $K$ son coprimos, $N \cap H = \{1_G\}$. A su vez, $o(G) = o(N)o(H) = o(N)o(K)$, luego por 3.3.4 se tendrá $G = NK$. Así, aplicando 1.2.1, exisistirá un homomorfismo $\phi : K \to Aut(N)$ tal que $G \cong N \rtimes_\phi K$. Q.E.D.

# Capítulo 3

# Generalidades sobre grupos

Después de lo dicho estamos casi listos para lanzarnos a la labor de determinar grupos. Vamos a terminar especificando algunas cuestiones técnicas, como los grupos de automorfismos de algunas de las familias de grupos más conocidas, propiedades de los grupos cíclicos o algunos resultados sobre isomorfía de grupos.

## 3.1. Grupos de automorfismos

Comencemos viendo los grupos de automorfismos de los grupos cíclicos cuando éstos son de orden potencia de un primo. Añadiendo a estos casos la proposición 3.1.5, por el teorema fundamental de la aritmética, tendremos el grupo de automorfismos de cualquier grupo cíclico. Omitimos las demostraciones por su extensión, pero pueden consultarse con facilidad en cualquier manual de teoría de grupos. En concreto, recomendamos [7].

**Proposición 3.1.1.** *Sean $p \in \mathbb{P}$ impar y $n \in \mathbb{N}$. Entonces $Aut(C_{p^n}) \cong C_{p^{n-1}(p-1)}$.*

**Proposición 3.1.2.** *Sea $n \in \mathbb{N}$. Entonces:*

- $Aut(C_{2^n}) \cong \{1_G\}$ *si* $n = 1$
- $Aut(C_{2^n}) \cong C_2$ *si* $n = 2$
- $Aut(C_{2^n}) \cong C_2 \times C_{2^{n-2}}$ *si* $n \geq 3$

Estudiemos ahora los automorfismos del grupo dihedral. Para más curiosidad, el resultado puede verse contextualizado en un marco distinto en [8].

**Proposición 3.1.3.** *Sea $n \in \mathbb{N}$, $n \geq 3$. Se da que*

$$Aut(D_n) \cong C_n \rtimes_\phi Aut(C_n),$$

*donde $\phi : Aut(C_n) \to Aut(C_n)$ es la identidad.*

*Demostración.* Denotemos $D_n \cong \langle\sigma\rangle \rtimes_\phi \langle\tau\rangle$, donde $\phi : C_2 \to Aut(C_n)$ viene dado por $\phi(\tau) = \eta$, cuando $\eta : C_n \to C_n : g \mapsto g^{-1}$; es decir, $D_n = \langle\sigma, \tau | \sigma^n = \tau^2 = 1_{D_n}, \tau\sigma\tau^{-1} = \sigma^{-1}\rangle$, como solemos manejar. Comenzaremos demostrando que $Aut(D_n)$ tiene un subgrupo normal isomorfo a $C_n$ y que la extensión

$$0 \longrightarrow C_n \longrightarrow Aut(D_n) \longrightarrow Aut(C_n) \longrightarrow 0$$

es separable. Finalmente, probaremos que el homomorfismo $\phi$ es la identidad.

Empecemos por hablar de qué forma tendrá un automorfismo de $D_n$. Nos basta, como acostumbramos, con definir la imagen de los generadores $\sigma$ y $\tau$, asegurándonos de que se respetan las restricciones algebraicas que éstos plantean (en este caso $\tau\sigma\tau^{-1} = \sigma^{-1}$) y se preserva el orden de dichos elementos. Dado entonces $\alpha \in Aut(D_n)$ tendremos que $o(\sigma) = o(\alpha(\sigma)) = n$ y, como $n > 2$, $\alpha(\sigma)$ no puede ser un elemento de la forma $\sigma^j\tau$ (todos ellos tienen orden dos), luego será uno de los elementos de orden $n$ en $\langle\sigma\rangle$, es decir, un $\sigma^i$, con $1 \leq i < n$ y $mcd(i,n) = 1$. A su vez, $\alpha(\tau)$ será un elemento de orden dos que no esté en $\langle\alpha(\sigma)\rangle$, pues $\tau \notin \langle\sigma\rangle$. Así, será uno cualquiera de los $\sigma^j\tau, 0 \leq j < n$; en efecto, en cualquier situación en que se de $\alpha(\tau) = \sigma^j\tau$ se mantendrá

$$\begin{aligned}\alpha(\tau\sigma\tau^{-1}) &= \alpha(\tau)\alpha(\sigma)\alpha(\tau^{-1}) = (\sigma^j\tau)(\sigma^i)(\sigma^j\tau)^{-1} \\ &= \sigma^j(\tau\sigma^i\tau^{-1})(\sigma^{-j}) = \sigma^j(\tau\sigma\tau^{-1})^i(\sigma^{-j}) \\ &= \sigma^j\sigma^{-i}\sigma^{-j} = \sigma^{-i} = \alpha(\sigma)^{-1}\end{aligned}$$

Llamaremos, a lo largo de la prueba, $\zeta_{x,y}$ al automorfismo de $D_n$ que manda $\sigma$ a $x$ y $\tau$ a $y$. Por lo dicho en el párrafo anterior, todo automorfismo será de la forma $\zeta_{\sigma^i,\sigma^j\tau}$, $1 \leq i < n, mcd(i,n) = 1$, $0 \leq j < n$. Consideremos $\zeta = \zeta_{\sigma,\sigma\tau}$, que envía cada $\sigma^i$ a sí mismo y cada $\sigma^i\tau$ a $\sigma^{i+1}\tau$. Éste es automorfismo porque envía cada elemento a otro de su mismo orden y respeta la propiedad $\tau\sigma\tau^{-1} = \sigma^{-1}$, todo lo mencionado en el párrafo anterior. Así, el subgrupo $\langle\zeta\rangle = \{\zeta_{\sigma,\sigma^i\tau} : 0 \leq i < n\}$ es de orden $n$. Además, éste es subgrupo normal, ya que dado otro $\alpha = \zeta_{\sigma^k,\sigma^l\tau} = \zeta_{\sigma^k,\tau} \circ \zeta_{\sigma,\sigma^l\tau} = \zeta_{\sigma^k,\tau}\zeta^l$ tenemos

$$\alpha\zeta\alpha^{-1} = (\zeta_{\sigma^k,\tau}\zeta^l)\zeta(\zeta_{\sigma^k,\tau}\zeta^l)^{-1} = \zeta_{\sigma^k,\tau}(\zeta^l\zeta\zeta^{-l})\zeta_{\sigma^k,\tau}^{-1} = \zeta_{\sigma^k,\tau}\zeta\zeta_{\sigma^k,\tau}^{-1} = \zeta_{\sigma,\sigma^j\tau} = \zeta^j \in \langle\zeta\rangle.$$

Es claro que además el cociente $Aut(D_n)/\langle\zeta\rangle$ es isomorfo a $Aut(C_n)$, pues cada clase de este cociente se describe simplemente por la imagen de $\sigma$, lo cual es como considerar $Aut(\langle\sigma\rangle) = Aut(C_n)$. Esto nos da la sucesión exacta (propia de un subgrupo normal):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_n & \xrightarrow{\ i\ } & Aut(D_n) & \xrightarrow{\ \pi\ } & Aut(C_n) & \longrightarrow & 0 \\ & & \sigma^i & \longmapsto & \zeta^i & \longmapsto & 1_{Aut(C_n)} & & \\ & & & & \zeta_{\sigma^i,\sigma^j\tau} & \longmapsto & (\sigma \mapsto \sigma^i) & & \end{array}$$

Ésta a su vez es escindida por el corte $\rho : Aut(C_n) \to Aut(D_n) : \omega \mapsto \zeta_{\omega(\sigma),\tau}$, pues es claro que es homomorfismo y, dado $\beta : C_n \to C_n : \sigma \mapsto \sigma^i$, se tiene $\pi \circ \rho(\beta) = \pi(\zeta_{\beta(\sigma),\tau}) = \beta$. Por ello, $Aut(D_n) \cong C_n \rtimes_\phi Aut(C_n)$, donde $\phi : Aut(C_n) \to Aut(C_n) : \beta \mapsto \beta$ porque la conjugación de $\zeta$ por $\zeta_{\sigma^j,\tau}$ resulta $\zeta^j$, como ya habíamos visto. Q.E.D.

El resultado siguiente también puede consultarse en [7].

**Proposición 3.1.4.** *Sean $n \in \mathbb{N}$ y $p \in \mathbb{P}$. Entonces $Aut(C_p \times \overset{n}{\ldots} \times C_p) \cong GL_n(\mathbb{F}_p)$*

Por último, conviene reseñar que, para dos grupos de orden coprimo, el grupo de automorfismos de su producto directo se puede descomponer en producto directo de los grupos de automorfismos de cada uno.

**Proposición 3.1.5.** *Sean $H$ y $K$ dos grupos finitos con $mcd(o(H), o(K)) = 1$. Entonces*

$$Aut(H \times K) \cong Aut(H) \times Aut(K).$$

*Demostración.* Sea la aplicación

$$\begin{array}{c} f : Aut(H) \times Aut(K) \longrightarrow Aut(H \times K) \\ \zeta = (\varphi, \psi) \longmapsto \left( \begin{array}{c} f(\zeta) : H \times K \to H \times K \\ (h,k) \mapsto (\varphi(h), \psi(k)) \end{array} \right) \end{array}$$

Queda claro que está bien definida, pues la aplicación imagen es un homomorfismo. Veamos que es isomorfismo.

Para ver que es homomorfismo sean $\zeta_1, \zeta_2 \in Aut(H \times K)$ y $(h,k) \in H \times K$. Con ello:

$$\begin{array}{l} (f(\zeta_1) \circ f(\zeta_2))(h,k) = f(\zeta_1)(\varphi_2(h), \psi_2(k)) = (\varphi_1(\varphi_2)(h), \varphi_1(\psi_2(k))) = \\ ((\varphi_1 \circ \varphi_2)(h), (\varphi_1 \circ \psi_2(k))) = f(\zeta_1\zeta_2)(h,k) \end{array}$$

Veamos ahora que es inyectiva, para lo cual nos basta con ver $ker(f) = \{1\}$. Sean $\zeta = (\varphi, \psi) \in ker(f)$ y $(h,k) \in H \times K$. Así: $f(\zeta)(h,k) = 1 \Rightarrow (\varphi(h), \psi(k)) = 1 \Rightarrow \varphi(h) = 1, \psi(k) = 1 \Rightarrow \varphi \equiv 1_H, \psi \equiv 1_K \Rightarrow \zeta \equiv 1_{H \times K}$.

Finalmente, para comprobar la sobreyectividad, sea $\omega \in Aut(H \times K)$ y busquemos un $\zeta \in Aut(H) \times Aut(K)$ tal que $f(\zeta) = \omega$. Consideremos, también, las proyecciones $\pi_H : H \times K \to H : (h,k) \mapsto h, \pi_K : H \times K \to K : (h,k) \mapsto k$. Miremos el homomorfismo

$$\begin{array}{ccccccc} \gamma_H : K & \overset{j}{\hookrightarrow} & H \times K & \overset{\omega}{\longrightarrow} & H \times K & \overset{\pi_H}{\longrightarrow} & H \\ k & \longmapsto & (1_H, k) & \longmapsto & \omega(1_H, k) & \longmapsto & \pi_H(\omega(1_H, k)) \end{array}$$

Con ello, por el primer teorema de isomorfía,

$$K/ker(\gamma_H) \cong Im(\gamma_H) < H \Rightarrow \frac{n}{o(\gamma_H)} \mid m \Rightarrow o(\gamma_H) = n \Rightarrow ker(\gamma_H) = K \Rightarrow \gamma_H \equiv 1_H$$

Análogamente el homomorfismo

$$\begin{array}{ccccccc} \gamma_K : H & \overset{i}{\hookrightarrow} & H \times K & \overset{\omega}{\longrightarrow} & H \times K & \overset{\pi_K}{\longrightarrow} & K \\ h & \longmapsto & (h, 1_K) & \longmapsto & \omega(h, 1_K) & \longmapsto & \pi_K(\omega(h, 1_K)) \end{array}$$

es idénticamente $1_K$. Llamemos así

$$\begin{array}{l} \omega_H : H \longrightarrow H : h \longmapsto \pi_H(\omega(h, 1_K)) \\ \omega_K : K \longrightarrow K : k \longmapsto \pi_K(\omega(1_H, k)) \end{array}$$

con lo que, si $\zeta = (\omega_H, \omega_K)$ y $(h,k) \in H \times K$, se tiene

$$\begin{array}{l} f(\zeta)(h,k) = (\omega_H(h), \omega_K(k)) = (\pi_H(\omega(h, 1_K)), 1_K)(1_H, \pi_K(\omega(1_H, k))) \\ = (\pi_H(\omega(h, 1_K)), \gamma_K(h))(\gamma_H(k), \pi_K(\omega(1_H, k))) \\ = (\pi_H(\omega(h, 1_K)), \pi_K(\omega(h, 1_K)))(\pi_H(\omega(1_H, k)), \pi_K(\omega(1_H, k))) \\ = (\pi_H(\omega(h, 1_K))\pi_H(\omega(1_H, k)), \pi_K(\omega(h, 1_K))\pi_K(\omega(1_H, k))) \\ = (\pi_H(\omega(h,k)), \pi_K(\omega(h,k))) = \omega(h,k) \\ \Rightarrow f(\zeta) = \omega \end{array}$$

Q.E.D.

## 3.2. Resultados sobre grupos cíclicos

Realizaremos ahora varias observaciones sobre la particularidad de los grupos cíclicos. Comencemos viendo que, para cada divisor del orden del grupo, un grupo cíclico sólo tiene un subgrupo de ese tamaño, y las repercusiones de esto a la hora de contar los elementos de un determinado orden.

**Proposición 3.2.1.** *Sea $G$ un grupo cíclico de orden finito. Para cada $m \in \mathbb{N} : m \mid o(G)$ existe un único $H < G$ tal que $o(H) = m$. Además, éste es cíclico.*

*Demostración.* Supongamos que $o(G) = n$ y $G = \langle g \rangle$. Tomemos $m \in \mathbb{N}$ tal que $m \mid n$, de forma que $n = dm, d \in \mathbb{N}$. Así, tomando el subgrupo $H = \langle g^d \rangle$ tenemos que éste tiene orden $m$, pues

$$o(H) = o(g^d) = \frac{n}{mcd(n,d)} = \frac{n}{d} = m$$

Veamos que éste es el único subgrupo de $G$ con orden $m$. Tomemos otro subgrupo $K < G$ de orden $m$. Los elementos de éste serán de la forma $g^k, k \in \mathbb{N}$, como todos los de $G$. Sea $k \in \mathbb{N}$ el mínimo de éstos cumpliendo que $g^k \neq 1_G$. Todo elemento $g^p \in K$ cumple que $k \mid p$ pues, dividiendo euclídeamente $p$ entre $k$, obtenemos que $p = qk + r$, con $q, r \in \mathbb{N}, 0 \leq r < k$, de tal modo que por la elección de $k$ se da que $r = 0$, y por tanto $k \mid p$. Con ello, $K = \langle g^k \rangle$, y, como la elección de $K$ es arbitraria, todo subgrupo de $G$ es cíclico.

Para ver que $H$ y $K$ coinciden basta ver que:

$$o(K) = o(g^k) = \frac{n}{mcd(n,k)} = \frac{n}{k} = m \Rightarrow k = \frac{n}{m} = d$$

Q.E.D.

**Corolario 3.2.2.** *Sea $G$ un grupo cíclico y sea $n \in \mathbb{N}$ tal que $n \mid o(G)$. Entonces $G$ tiene $\varphi(n)$ elementos de orden $n$, donde $\varphi$ es la función phi de Euler.*

*Demostración.* Como por 3.2.1 $G$ solo tiene un elemento de orden $n$, en éste estarán todos los elementos de orden $n$. Además, si $g \in G$ es un elemento de orden $n$ (y por tanto generador de dicho subgrupo), entonces todos los elementos de orden $n$ serán de la forma $g^i$, para $i \in \{1, ..., n-1\}$ tal que $mcd(i, n) = 1$. Con ello, la cantidad de elementos de orden $n$ en $G$ se corresponderá con la cantidad de naturales $i$ menores que $n$ y coprimos con él, que es $\varphi(n)$. Q.E.D.

La propiedad que nos va a resultar más interesante de los grupos cíclicos de orden par va a ser que tienen un único elemento de orden dos. La existencia de este elemento no es para nosotros ninguna sorpresa, pero su unicidad será algo que deberemos tener en cuenta al buscar elementos de orden dos en grupos.

**Corolario 3.2.3.** *Sea $G$ un grupo cíclico de orden finito y par. Entonces existe un único $\eta \in G$ tal que $o(\eta) = 2$.*

*Demostración.* Basta aplicar 3.2.2 teniendo en cuenta que $\varphi(2) = 1$. Q.E.D.

Es también bien conocida la relación del producto directo con la familia de grupos cíclicos a la hora de descomponer en factores coprimos.

**Proposición 3.2.4.** *Sean $n, m \in \mathbb{N}$ tales que $mcd(m, n) = 1$. Entonces $C_{mn} = C_m \times C_n$*

*Demostración.* Consideremos $C_m = \langle a \rangle$ y $C_n = \langle b \rangle$. Busquemos en $C_m \times C_n$ un elemento de orden $mn$ y habremos terminado. Tomemos $x = (a, b) = (a, 1_{C_n})(1_{C_m}, b) \in C_m \times C_n$. Sabemos que tanto $C_m$ como $C_n$ son abelianos, con lo que también lo es $C_m \times C_n$. Como en todo grupo abeliano, el orden del producto de dos elementos es el mínimo común múltiplo de los órdenes de los dos elementos. Así,

$$\begin{aligned} o(x) &= o((a, 1_{C_n})(1_{C_m}, b)) = mcm(o(a, 1_{C_n}), o(1_{C_m}, b)) \\ &= mcm(o(a), o(b)) = \frac{o(a)o(b)}{mcd(o(a), o(b))} = mn, \end{aligned}$$

con lo que ya lo tenemos. Q.E.D.

## 3.3. Otras generalidades sobre grupos

En esta última sección introducimos el resto de resultados técnicos que nos serán necesarios más adelante.

**Lema 3.3.1.** *Sea $H < Z(G)$ tal que $G/H$ es cíclico. Entonces $G$ es abeliano.*

*Demostración.* Como $H \subset Z(G)$, los elementos de $H$ conmutan con todos los elementos de $G$, con lo que $H \triangleleft G$ y el cociente $G/H$ es grupo. Además, si $G/H$ es cíclico, también lo es $\frac{G/H}{Z(G)/H}$, y como por el segundo teorema de isomorfía

$$G/Z(G) \cong \frac{G/H}{Z(G)/H}$$

también es cíclico $G/Z(G)$, es decir, $\exists g \in G : G/Z(G) = \langle gZ(G) \rangle$. Llamemos $r = o(gZ(G))$. Con esto, dado $a \in G$ existen $m \in \{0, ..., r-1\}$, $z \in Z(G)$ tales que $a = g^m z$. De este modo, dados $a_1, a_2 \in G$ con $a_1 = g^{m_1} z_1$ y $a_2 = g^{m_2} z_2$ tenemos, por pertenecer $z_1$ y $z_2$ al centro:

$$a_1 a_2 = g^{m_1} z_1 g^{m_2} z_2 = z_2 g^{m_1} g^{m_2} z_1 = z_2 g^{m_2} g^{m_1} z_1 = g^{m_2} z_2 g^{m_1} z_1 = a_2 a_1$$

con lo que $G$ es abeliano. Q.E.D.

**Lema 3.3.2.** *Sea $G$ un grupo de orden $n$ y sea $k \in \mathbb{N}$ el divisor de $n$ más pequeño distinto de uno. Si $H < G$ un subgrupo tal que $[G : H] = k$, entonces $H \triangleleft G$.*

La demostración del resultado puede consultarse en [4]. No obstante, lo explicitamos por el número de veces que haremos uso de él.

**Lema 3.3.3.** *Sean $G$ un grupo, $N \triangleleft G$ un subgrupo normal abeliano y $h \in G \setminus N$. Tomemos el homomorfismo $\varphi : N \to N : n \mapsto hnh^{-1}$. Entonces $o(\varphi) \mid [G : N]$.*

*Demostración.* Puesto que $h \notin N$, $hN$ no es el elemento neutro de $G/N$, con lo que tomemos $k = o(hN)$, es decir, tal que $h^k \in N$. Con esto tenemos que $\varphi^k = 1_{Aut(N)}$, puesto que, como $N$ es abeliano y $h^k \in N$, se tiene que $\varphi^k(n) = h^k n h^{-k} = n, \forall n \in N$. Así pues, $o(\varphi) \mid k$, pero como $k = o(hN) \mid o(G/N) = [G : N]$ tenemos que $o(\varphi) \mid [G : N]$. Q.E.D.

**Proposición 3.3.4.** *Sea $G$ un grupo finito y sean $H$ y $K$ subgrupos de $G$ tales que*

$$mcd(o(H), o(K)) = 1, H \cap K = \{1_G\}, o(H)o(K) = o(G).$$

*Entonces $G = HK$.*

*Demostración.* Sabemos que $HK = \{hk : h \in H, k \in K\}$. Además, cada elemento $hk$ en $HK$ tiene una representación única como producto de un elemento de $H$ y uno de $K$. En efecto, si $h_1k_1 = h_2k_2$, con $h_1, h_2 \in H$ y $k_1, k_2 \in K$, entonces $h_1^{-1}h_2 = k_1k_2^{-1}$, y este elemento estará tanto en $H$ como en $K$, luego será, por hipétesis, $1_G$, de forma que $h_1 = h_2$ y $k_1 = k_2$. Por lo tanto habrá en $HK$ tantos elementos como parejas $(h, k)$, que son $o(H)o(K)$ en total. Tenemos pues que $HK \subset G$, y el cardinal de ambos conjuntos coincide, luego $G = HK$. Q.E.D.

Estos dos últimos resultados acerca de la isomorfía serán útiles y usados en el capítulo 5.

**Lema 3.3.5.** *Sea $G = \langle x, x_1, .., x_n\rangle$ un grupo con $\langle x\rangle \cap \langle x_1, ..., x_n\rangle = \{1_G\}$ y $xx_i = x_ix$ para todo $i \in \{1, ..., n\}$. Entonces $G \cong \langle x\rangle \times \langle x_1, ..., x_n\rangle$.*

*Demostración.* Consideremos la aplicación

$$\begin{aligned} f : \langle x, x_1, ..., x_n\rangle &\longrightarrow \langle x\rangle \times \langle x_1, ..., x_n\rangle \\ x &\longmapsto (x, 1) \\ x_i &\longmapsto (1, x_i). \end{aligned}$$

Está bien definida porque $\langle x\rangle \cap \langle x_1, ..., x_n\rangle = \{1_G\}$, y es homomorfismo porque dados $a, b \in G$ con $a = x^iy_i$ y $b = x^jy_j$ en G, con $y_i, y_j \in \langle x_1, ..., x_n\rangle$ tenemos, dado que $x$ y $x_i$ conmutan, que

$$\begin{aligned} f(ab) &= f(x^iy_ix^jy_j) \\ &= f(x^ix^jy_iy_j) \\ &= (x^i, 1)(x^j, 1)(1, y_i)(1, y_j) \\ &= (x^i, 1)(1, y_i)(x^j, 1)(1, y_j) \\ &= (x^i, y_i)(x^j, y_j) \\ &= f(a)f(b). \end{aligned}$$

La aplicación es inyectiva porque, tomando los $a$ y $b$ anteriores,

$$f(a) = f(b) \Rightarrow (x^i, y_i) = (x^j, y_j) \Rightarrow i = j, y_i = y_j \Rightarrow a = b.$$

La aplicación es sobreyectiva porque dado un $b = (x^i, y_i) \in \langle x\rangle \times \langle x_1, ..., x_n\rangle$, podemos tomar $a = x^iy_i$ de tal modo que $f(a) = b$. Q.E.D.

**Proposición 3.3.6.** *Sea $n \in \mathbb{N}$ impar. Entonces $D_{2n} \cong C_2 \times D_n$.*

*Demostración.* Digamos que $C_2 = \{1_{C_2}, \eta\}$ y $D_n = \langle \sigma, \tau | \sigma^n = \tau^2 = 1_{D_n}, \tau\sigma\tau^{-1} = \sigma^{-1}\rangle$. Tomemos los elementos $g = (\eta, \sigma)$ y $h = (1_{C_2}, \tau)$ en $C_2 \times D_n$. Es claro que $o(h) = 2$; también se comprueba con facilidad que, como $g = (\eta, 1_{D_n})(1_{C_2}, \sigma) = (1_{C_2}, \sigma)(\eta, 1_{D_n})$, el orden de $g$ es el mínimo común múltiplo de los órdenes de $\eta$ y $\sigma$ que, puesto que $n$ es impar, es $2n$. Finalmente,

$$hgh^{-1} = (1_{C_2}, \tau)(\eta, \sigma)(1_{C_2}, \tau^{-1}) = (\eta, \tau\sigma\tau^{-1}) = (\eta^{-1}, \sigma^{-1}) = g^{-1},$$

lo que nos da el isomorfismo buscado. Q.E.D.

# Capítulo 4

# Resultados de determinación

Ahora que tenemos herramientas para ello, podemos pasar a la parte práctica del trabajo. Vamos a proceder a clasificar y determinar grupos, eligiendo sus órdenes u órdenes de algunos de sus elementos adecuadamente para poderlos manipular con facilidad.

Comenzaremos viendo los grupos de orden potencia de un primo y seguiremos con los de orden $kp$, con $k \in \mathbb{N}$ pequeño y determinado.

## 4.1. Órdenes $p$ y $p^2$

Comencemos por órdenes de un grupo finito sencillos: $p$ y $p^2$. El primero es corolario directo del teorema de Lagrange, aunque el segundo requiere de la primera intervención del producto semidirecto.

**Teorema 4.1.1.** *Sea $G$ un grupo de orden $p \in \mathbb{P}$. Entonces $G \cong C_p$.*

*Demostración.* Dado $g \in G$, por el teorema de Lagrange, $o(g) \mid p$. Claro que, tomando $g \neq 1_G$, tenemos que $o(g) = p$ y por tanto $G = \langle g \rangle$, luego $G \cong C_p$. Q.E.D.

**Teorema 4.1.2.** *Sea $G$ un grupo de orden $p^2$, con $p \in \mathbb{P}$. Entones $G \cong C_{p^2}$ o $G \cong C_p \times C_p$.*

*Demostración.* Por el teorema de Lagrange, los elementos de $G$ distintos de la unidad pueden tener orden $p$ o $p^2$. Si al menos uno de ellos tiene orden $p^2$ entonces, y sólo entonces, el grupo es cíclico e isomorfo a $C_{p^2}$. Si, por el contrario, todos los elementos de $G$ distintos de la unidad tienen orden $p$, por el primer teorema de Sylow sabemos que existe $N \triangleleft G$ con $o(N) = p$. Si además tomamos $h \in G \setminus N$, éste tendrá orden $p$, $\langle h \rangle \cap N = \{1_G\}$ y, debido a 3.3.4, $\langle h \rangle N = G$, de modo que, por 1.2.1, existirá un único homomorfismo $\phi : \langle h \rangle \to Aut(N)$ tal que $G \cong N \rtimes_\phi \langle h \rangle$. También es cierto que $Aut(N) \cong C_{p-1}$ por 3.1.1 y, teniendo en cuenta que $p - 1 \nmid p = o(h)$, necesariamente $\phi(h) = 1_{Aut(N)}$, con lo que $\phi \equiv 1_{Aut(N)}$. Por 1.3.1, $G \cong C_p \times C_p$. Q.E.D.

## 4.2. Orden $p^3$

El grupo de orden $p^3$, pese a tener tan solo cinco determinaciones posibles, nos va a resultar algo más complicado de especificar. Los lemas que se exponen a continuación nos harán la tarea más sencilla.

**Lema 4.2.1.** *Sea $G$ un grupo no abeliano de orden $p^3, p \in \mathbb{P}$, y sea $Z$ su centro. Entonces:*

- $o(Z) = p$

- $G/Z \cong C_p \times C_p$
- $[G,G] = Z$.

*Demostración.* Como $G$ es un $p$-grupo de Sylow no trivial, su centro es no trivial. Así, $o(Z) \in \{p, p^2, p^3\}$. No puede ser $o(Z) = p^3$ porque en tal caso $G$ sería abeliano. Por 3.3.1, si $G/Z$ es cíclico entonces $G$ es abeliano, con lo que no puede ser $o(G/Z) = p$. Con ello, $o(Z) = p$. Además, $o(G/Z) = p^2$, y sabemos por 4.1.2 que sólo hay dos grupos con este orden, y uno de ellos es el cíclico, con lo que necesariamente ha de ser el otro, de modo que $G/Z \cong C_p \times C_p$. Finalmente, como $G/Z$ es abeliano, $[G,G] \subset Z$, y como $[G,G]$ no es trivial, pues $G$ no es abeliano, se da que $Z = [G,G]$. Q.E.D.

**Lema 4.2.2.** *Sea $G$ un grupo y sean $x, y \in G$ que conmuten con $[x,y]$. Entonces:*

$$x^n y^n = (xy)^n [x,y]^{\binom{n}{2}}, \forall n \in \mathbb{N} \setminus \{1\}$$

*Demostración.* Demostramos por inducción sobre $n \in \mathbb{N} \setminus \{1\}$. Si $n = 2$ tenemos:

$$x^2y^2 = xxyy = xxy(x^{-1}y^{-1}yx)y = x(xyx^{-1}y^{-1})yxy = xyxy(xyx^{-1}y^{-1}) = (xy)^2[x,y]^{\binom{2}{2}}.$$

Ahora, suponiéndolo para $n$ lo demostramos para $n+1$. Teniendo en cuenta que $\binom{n+1}{2} = \binom{n}{1} + \binom{n}{2} = n + \binom{n}{2}$, podemos desarrollar:

$$(xy)^{n+1}[x,y]^{\binom{n+1}{2}} = (xy)^{n+1}[x,y]^n[x,y]^{\binom{n}{2}} = x([x,y]yx)^n y[x,y]^{\binom{n}{2}} = x(xyx^{-1}y^{-1}yx)^n y[x,y]^{\binom{n}{2}}$$
$$= x(xy)^n y[x,y]^{\binom{n}{2}} = x(xy)^n[x,y]^{\binom{n}{2}}y = xx^n y^n y = x^{n+1}y^{n+1},$$

con lo que queda demostrado. Q.E.D.

**Lema 4.2.3.** *Sea $G$ un grupo no abeliano de orden $p^3$, con $p \in \mathbb{P} \setminus \{2\}$. Entonces existen $N \triangleleft G$, $h \in G \setminus N$ tales que $o(N) = p^2$ y $o(h) = p$.*

*Demostración.* Comencemos diciendo que por 3.3.2, cualquier subgrupo de $G$ de orden $p^2$ va a ser normal. Como $G/Z \cong C_p \times C_p$, tal y como se indicaba en 4.2.1, podemos tomar $x, y \in G$ tales que $G/Z = \langle \overline{x}, \overline{y} \rangle$. Tengamos en cuenta que ninguno de los dos es el neutro de $G$ y que $\langle x \rangle \cap \langle y \rangle = \{1_G\}$. Al no ser $G$ abeliano no puede ser cíclico, con lo que los elementos no triviales de $G$ tienen orden $p$ o $p^2$.

No puede darse que $x$ e $y$ conmuten, pues en tal caso $G$ sería abeliano, con lo que $[x,y] \neq 1_G$, y como además $[x,y] \in [G,G] = Z$, de nuevo por 4.2.1, tenemos $Z = \langle [x,y] \rangle$, y por tanto $G = \langle x, y, [x,y] \rangle = \langle x, y \rangle$. Llamaremos, en adelante, $z = [x,y]$. Claramente $o(z) = p$.

Vamos, pues, a buscar el subgrupo $N$ y el elemento $h$ deseados. Si tanto $x$ como $y$ tienen orden $p$, nos basta considerar $N = \langle x, z \rangle$ y $h = y$, de manera que $h \notin N$.

Antes de continuar, veamos que $g^p \in Z, \forall g \in G$. En efecto, si $g \in G$, podemos considerar $\overline{g} \in G/Z \cong C_p \times C_p$, donde todo elemento no neutro tiene orden $p$, con lo que $\overline{g}^p = 1_{G/Z}$, es decir, $g^p \in Z$.

Consideremos ahora que uno de los elementos $x$ o $y$ tiene orden $p^2$, sin pérdida de generalidad $y$. Si $o(x) = p$, ya lo tenemos, pues nos basta tomar $N = \langle y \rangle$ y $h = x$ de tal modo que $o(N) = p^2$, $o(h) = p$ y $h \notin N$ porque $x \notin \langle y \rangle$.

Ahora bien, si $o(x) = p^2$, sabemos que $y^p \in Z$, y $o(y) = p^2$, con lo que $o(y^p) = p$ y $Z = \langle y^p \rangle$. También $x^p \in Z = \langle y^p \rangle$, de forma que $\exists r \in \{1, ..., p-1\}$ tal que $x^p = (y^p)^r$. De este modo, en virtud de 4.2.2 y que $p \neq 2$ (y por lo tanto $p \mid \binom{p}{2}$) se da:

$$x^p = (y^p)^r \Rightarrow x^p(y^{-r})^p = 1_G \Rightarrow (xy^{-r})^p[x,y]^{\binom{p}{2}} = 1_G \Rightarrow (xy^{-r})^p = 1_G.$$

Además $xy^{-r} \neq 1_G$ porque $x \notin \langle y \rangle$, con lo que $o(xy^{-r}) = p$. Con todo ello, $G = \langle x, y \rangle = \langle xy^{-r}, y \rangle$, y por tanto podemos tomar $N = \langle y \rangle$, $h = xy^{-r}$, y de este modo tenemos de nuevo el resultado buscado. Q.E.D.

Nótese que cuando $p = 2$, en el proceso anterior, no se da $2 \mid \binom{2}{2}$, con lo que no podemos garantizar la existencia de dicho subgrupo y dicho elemento.

Los siguientes dos lemas describen los dos grupos de orden $p^3$ que no son abelianos en el caso en que $p \neq 2$, que simplemente enlazaremos con el siguiente resultado, que clasifica estos mismos grupos.

**Lema 4.2.4.** $C_{p^2} \rtimes C_p \cong \langle x, t | x^{p^2} = t^p = 1, xt = tx^{p+1} \rangle$, $p \in \mathbb{P}$.

*Demostración.* Sean $N = C_{p^2} = \langle g \rangle, H = C_p = \langle h \rangle$ y $\beta : C_{p^2} \to C_{p^2} : g \mapsto g^{p+1}$, que claramente es un automorfismo. Teniendo en cuenta:

$$(p+1)^{p+1} = \sum_{i=0}^{p+1} \binom{p+1}{i} p^i \overset{p^2}{\equiv} \binom{p+1}{0} + \binom{p+1}{1} p = 1 + p(p+1) \overset{p^2}{\equiv} 1 + p \tag{4.1}$$

tenemos que $o(\beta) = p$:

$$\beta^{p+1}(g) = g^{(p+1)^{p+1}} \overset{(4,1)}{=} g^{p+1} \Rightarrow \beta^{p+1} = \beta \Rightarrow \beta^p = 1_{Aut(C_{p^2})}$$

Consideremos entonces $\phi : C_p \to Aut(C_{p^2}) : a \mapsto \beta^{-1}$. Veamos que $C_{p^2} \rtimes_\phi C_p$ sigue la descripción dada. Sean $x = (g, 1_H), t = (1_N, h)$ elementos de $N \times H$ que generan $N \rtimes_\phi H$. Finalmente, con ello:

$$xt = (g, 1_H)(1_N, h) = (g, h)$$

$$tx^{p+1} = (1_N, h)(g, 1_H)^{p+1} = (1_N, h)(g^{p+1}, 1_H) = (\beta^{-1}(g^{p+1}), h) = (\beta^{-1}(\beta(g)), h) = (g, h)$$

con lo que ya tenemos el isomorfismo. Q.E.D.

**Lema 4.2.5.** $(C_p \times C_p) \rtimes C_p \cong \langle x, y, z | [x, y] = z, [x, z] = [y, z] = 1, x^p = y^p = z^p = 1 \rangle$.

*Demostración.* Consideremos $C_p = \langle g \rangle$ y el automorfismo:

$$\begin{array}{c} \zeta : C_p \times C_p \longrightarrow C_p \times C_p \\ (a, b) \longmapsto (ab, b) \end{array}$$

y por tanto $\zeta^n(a, b) = (ab^n, b)$, con lo que $o(\zeta) = p$. De este modo el homomorfismo $\phi : C_p \to Aut(C_p \times C_p) : g \mapsto \zeta$ define el producto semidirecto.

Debemos ver que la elección de $\zeta$ como imagen de $h$ por $\phi$ no resta generalidad. Sabemos que $Aut(C_p \times C_p) \cong GL_2(\mathbb{F}_p)$ tiene dos subgrupos de orden $p$, el generado por $(a, b) \mapsto (a^s, b)$, donde $s$ es cualquier generador de $\mathbb{F}_p^\times$, y $\zeta$. Si tomamos como imagen de $h$ por $\phi$ a cualquiera generado por el primero, teniendo en cuenta el isomorfismo inverso a $\beta : H \to H : g \mapsto g^s$ tendremos, por 1.2.2, que $(C_p \times C_p) \rtimes C_p \cong C_p \times C_p \times C_p$, que no es lo que venimos buscando. Respecto a los otros automorfismos, los generados por $\zeta$, tomemos otro isomorfismo $\psi : C_p \to Aut(C_p \times C_p) : g \mapsto \delta$, con $o(\delta) = p$, tal que $\langle \zeta \rangle = \langle \delta \rangle$. Existirá por tanto un $k \in \{1, ..., p-1\}$ tal que $\delta^k = \zeta$. Teniendo en cuenta que $C_p = \langle g \rangle = \langle g^k \rangle$, tenemos que $\beta : H \to H : g \mapsto g^k$ es automorfismo. Con ello, $\psi(\beta(g)) = \psi(g^k) = (\psi(g))^k = \delta^k = \zeta = \phi(g)$, con lo que $\phi = \psi \circ \beta$. Aplicando el resultado 1.2.2 tenemos

$$(C_p \times C_p) \rtimes_\psi C_p = (C_p \times C_p) \rtimes_{\psi \circ \beta} C_p = (C_p \times C_p) \rtimes_\phi C_p,$$

de modo que la elección de $\zeta$ no resta generalidad al producto semidirecto.

Tomemos entonces $x, y, z \in (C_p \times C_p) \rtimes C_p$ de la forma

$$x = ((1,1),g)$$

$$y = ((1,g),1)$$

$$z = ((g,1),1),$$

de modo que generan $(C_p \times C_p) \rtimes C_p$ y es inmediato comprobar que

$$[x,y] = ((1,1),g)((1,g),1)((1,1),g^{-1})((1,g^{-1}),1) = ((g,1),1) = z$$

$$[x,z] = ((1,1),g)((g,1),1)((1,1),g^{-1})((g^{-1},1),1) = ((1,1),1) = 1$$

$$[y,z] = ((1,g),1)((g,1),1)((1,g^{-1}),1)((g^{-1},1),1) = ((1,1),1) = 1$$

$$x^p = ((1,1),g)^p = ((1,1),g^p) = ((1,1),1) = 1$$

$$y^p = ((1,g),1)^p = ((1,g^p),1) = ((1,1),1) = 1$$

$$z^p = ((g,1),1)^p = ((g^p,1),1) = ((1,1),1) = 1,$$

con lo que ya tenemos el isomorfismo. Q.E.D.

**Teorema 4.2.6.** *Sea $G$ un grupo de orden $p^3$, con $p \in \mathbb{P}$. Entonces $G$ es isomorfo a uno de los siguientes grupos:*

- $C_{p^3}$
- $C_{p^2} \times C_p$
- $C_p \times C_p \times C_p$
- $C_{p^2} \rtimes C_p = \langle x,t | x^{p^2} = t^p = 1, xt = tx^{p+1} \rangle$
- $(C_p \times C_p) \rtimes C_p = \langle x,y,z | [x,y] = z, [x,z] = [y,z] = 1, x^p = y^p = z^p \rangle$

*Demostración.* Por el teorema de clasificación de los grupos abelianos finitos, los tres primeros serán los únicos grupos abelianos de orden $p^3$ posibles, y por tanto sólo debemos buscar los grupos no abelianos. En éste caso, por 4.2.3, existe $N \lhd G$ con $o(N) = p^2$ y $h \in G \setminus N$ tal que $h^p = 1_G$.

Así, tomando $H = \langle h \rangle$ tenemos, por 1.2.1, que hay un homomorfismo $\phi : \langle g \rangle \to Aut(H)$ tal que $G \cong H \rtimes_\phi \langle g \rangle$. Veamos gracias a él las distintas posibilidades de $G$. Sabemos, por 4.1.2, que $G \cong C_{p^2}$ o $G \cong C_p \times C_p$.

Si $N \cong C_{p^2}$, $\phi(h)$ puede tener orden 1 o $p$. Si tiene orden 1, por 1.3.1, $G \cong C_p \times C_{p^2}$ y, si tiene orden $p$, por 4.2.4, $G \cong C_{p^2} \rtimes C_p$.

Si $N \cong C_p \times C_p$, $\phi(h)$ puede tener orden 1 o $p$. Si tiene orden 1, por 1.3.1, $G \cong C_p \times C_p \times C_p$ y, si tiene orden $p$, por 4.2.5, $G \cong (C_p \times C_p) \rtimes C_p$. Q.E.D.

No podemos terminar esta sección sin mencionar lo que sucede cuando $p = 2$. Es innegable que los tres grupos abelianos se mantienen intactos, pero no sucede así para los dos grupos no abelianos. Si nos fijamos en la descripción del quinto grupo, establecida en 4.2.5, encontramos que $(C_2 \times C_2) \rtimes C_2 = \langle x,y,z | x^2 = y^2 = z^2 = 1, (xy)^2 = z, xz = zx, yz = zy \rangle$. Así pues, los elementos $x,y,z$ son de orden dos, de modo que son su propio inverso, y tomando los elementos $v = xy$ y $w = yz$ tenemos que $v^2 = z$, con lo que $v$ es de orden 4, y $w$ es de orden 2 porque $y$ y $z$ conmutan. Además, $wvw^{-1} = (yz)(xy)(yz) = yzxy^2z = yzxz = yxz^2 = yx = v^{-1} = v^3$, de forma que esta descripción coincide con la de $C_4 \rtimes C_2$ dada en 4.2.4, y por tanto los dos grupos son isomorfos. No es esfuerzo darse cuenta de que este grupo es $D_4$.

No obstante aparece en escena otro grupo no abeliano distinto al dihedral, que completará la lista: el primero de los dicíclicos, $DC_2$, al que como es costumbre llamaremos grupo cuaternión, $Q$.

Para la siguiente demostración, por aquello que vimos en el ejemplo 2.2.1, deberemos abstenernos de buscar subgrupos que nos den un producto semidirecto.

**Teorema 4.2.7.** *Sea $G$ un grupo de orden 8. Entonces $G$ es isomorfo a uno de los siguientes grupos:*

- $C_8$
- $C_4 \times C_2$
- $C_2 \times C_2 \times C_2$
- $D_4 = \langle x, t | x^4 = t^2 = 1, txt^{-1} = x^{-1} \rangle$
- $Q = \langle i, j | i^4 = j^4 = 1, jij^{-1} = i^{-1} \rangle$.

*Demostración.* Procedemos de un modo similar a 4.2.6. Los elementos en $G$ pueden ser de órdenes 1, 2, 4 u 8. Si lo hay de orden 8 el grupo será cíclico, el primer grupo del enunciado.

Supongamos pues que no hay elementos de orden 8, de forma que puede ser que haya elementos de orden 4 o que no. Si no los hay, todos los elementos distintos del neutro serán de orden 2, con lo que podemos encontrar un subgrupo isomorfo a $C_2 \times C_2$ y un elemento de orden 2 fuera de este, lo que nos dará, en virtud de 1.2.1, el grupo tercero del enunciado.

Ahora bien, si hay elementos de orden 4, por ejemplo $g \in G$, caben dos posibilidades: que todos los elementos de orden 2 estén en $\langle g \rangle$ o que podamos encontrar uno en $G \setminus \langle g \rangle$. Si hay uno fuera, de nuevo podemos aplicar 1.2.1 para encontrar los grupos segundo y cuarto del enunciado.

Si todos los elementos de orden 2 están en $\langle g \rangle$, cualquier $h \in G \setminus \langle g \rangle$ que tomemos tendrá orden cuatro. Necesariamente $G = \langle g, h \rangle$, pues $\langle g \rangle \subsetneq \langle g, h \rangle$ y $[G : \langle g \rangle] = 2$. Además, por 3.3.2, $\langle g \rangle \triangleleft G$, de modo que $hgh^{-1} \in \langle g \rangle$, y éste debe ser de orden 4, con lo que sólo se puede dar $hgh^{-1} = g$ o $hgh^{-1} = g^{-1}$. Claro que el primer caso nos llevaría a que $G$ es abeliano, y la isomorfía a cualquiera de los grupos abelianos de orden 8 contradiría una de las hipótesis que le hemos supuesto a $G$ a lo largo del proceso (no hay elementos de orden 8, no hay elementos de orden 4 con un elemento de orden 2 no generado por éstos y hay elementos de orden 4; respectivamente en el orden del enunciado), de modo que $hgh^{-1} = g^{-1}$ y hemos encontrado la presentación del quinto grupo. Q.E.D.

## 4.3. Órdenes múltiplos de primos

En esta sección analizaremos los grupos de orden $2p$, $4p$ y $pq$, atendiendo a la divisibilidad relativa de $p$ y $q$, lo que nos dará como colorarios $3p$ y $5p$.

Comenzando por $2p$, veamos que sólo tiene dos posibilidades no isomorfas: el grupo clíclico y el dihedral. Además, estos son fácilmente discernibles atendiendo a que uno es abeliano y el otro no.

**Teorema 4.3.1.** *Sea $G$ un grupo de orden $2p$, con $p \in \mathbb{P}$. Entonces $G \cong C_{2p}$ o $G \cong D_p$.*

*Demostración.* Por el teorema de Cauchy, $\exists g, h \in G : o(g) = p, o(h) = 2$. Llamemos $N = \langle g \rangle, H = \langle h \rangle$. Como $o(h) \nmid o(p)$, se tiene $h \notin \langle g \rangle$. También $[G : \langle g \rangle] = 2$, con lo que $\langle g \rangle \triangleleft G$ en virtud de 3.3.2. Es claro con esto que $H \cap N = 1_G$ y $HN = G$, de modo que, por 1.2.1, se da $\exists \phi : H \to Aut(N) : G \cong \langle g \rangle \rtimes_\phi \langle h \rangle$. Las posibilidades de $G$ vendrán determinadas por las posibilidades de $\phi(h)$.

Como $\langle g\rangle \cong C_p$, por 3.1.1, $Aut(N) \cong C_{p-1}$, de modo que, por 3.2.3, existirá un único elemento $\eta \in Aut(N)$ de orden dos, que por supuesto cumplirá $\eta(x) = x^{-1}, \forall x \in N$. Es necesario que $o(\phi(h)) \mid o(h)$, con lo que $o(\phi(h)) \in \{1, 2\}$.

Si $o(\phi(h)) = 1$, entonces $\phi(h) = 1_{Aut(\langle g\rangle)}$, y por 1.3.1, $G \cong H \times N \cong C_2 \times C_p \cong C_{2p}$.

Si $o(\phi(h)) = 2$, entonces $\phi(h) = \eta$. En este caso, tomemos de $N \times H$ los elementos $\sigma = (g, 1_G), \tau = (1_G, h)$, con lo que es claro que $o(\sigma) = p, o(\tau) = 2$ y, operando:

$$\sigma\tau = (g, 1_H)(1_N, h) = (g\phi(1_H)(1_N), 1_H h) = (g, h) = (1_N\eta(g^{-1}), h1_H) =$$
$$(1_N\phi(h)(g^{-1}), h1_H) = (1_N, h)(g^{-1}, 1_H) = (1_N, h)(g, 1_H)^{-1} = \tau\sigma^{-1}$$

Con lo que ya tenemos $G \cong D_p$. Q.E.D.

Finalmente, los grupos de orden $4p$ nos hacen darnos cuenta de las particularidades y detalles a tener en cuenta cuando operamos con productos semidirectos y grupos de automorfismos.

**Teorema 4.3.2.** *Sea $G$ un grupo de orden $4p$, con $p \in \mathbb{P}$, $p > 3$. Entonces, $G$ es isomorfo a uno de los siguientes grupos:*

- $C_{4p}$
- $C_{2p} \times C_2$
- $D_{2p} = \langle \sigma, \tau : \sigma^{2p} = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1}\rangle$
- $DC_p = \langle x, t : x^{2p} = 1, t^2 = x^p, xt = tx^{-1}\rangle$
- $E_p = \langle x, t : x^p = 1, t^4 = 1, txt^{-1} = \zeta(x)\rangle$

*dándose esta última sólo cuando $4 \mid p-1$, siendo $\zeta \in Aut(C_p)$ uno de los elementos de orden 4.*

*Demostración.* Por el primer teorema de Sylow $\exists g \in G : o(g) = p$, de modo que llamamos $N = \langle g\rangle$. Además, $N \lhd G$, pues, por el tercer teorema de Sylow, $n_p \equiv 1(p)$, pero es claro que no puede haber $p+1$ subgrupos de orden $p$, pues $(p-1)(p+1)+1 > 4p$. También, por el primer teorema de Sylow $\exists H < G : o(H) = 4$. Como $mcd(4, p) = 1$, por el teorema de Lagrange, $H \cap N = \{1_G\}$ y, por 3.3.4, $HN = G$ luego, de nuevo por el teorema 1.2.1, $\exists \phi : H \to Aut(N) : G \cong N \rtimes_\phi H$. Veamos los distintos casos de $H$ y $\phi$ para ver que resultan los distintos casos de grupos. Tengamos en cuenta que $Aut(N) \cong C_{p-1}$, por 3.1.1, con un único elemento de orden dos, dado 3.2.3, al que llamaremos $\eta$.

Consideremos $H \cong C_2 \times C_2$, con $C_2 = \{0, 1\}$. Si $\phi \equiv 1_{Aut(N)}$, por 1.3.1, $G \cong C_{2p} \times C_2$. Si, por el contrario, al menos un elemento $h \in H \setminus \{1_H\}$ cumple $\phi(h) \neq 1_{Aut(N)}$, como $o(\phi(h)) \mid o(h)$ y $h \neq 1_H$, necesariamente $\phi(h) = \eta$. Como además $H$ está generado por cualesquiera dos de sus elementos no neutros, se tendrá que dos de ellos tienen como imagen por $\phi$ a $\eta$. Consideremos, sin pérdida de generalidad (por 1.2.2), que éstos son $(1, 0)$ y $(0, 1)$.

Veamos que en este caso $G \cong D_{2p}$. Sean $\sigma = (g, (1, 1))$ y $\tau = (1_N, (1, 0))$ elementos de $N \rtimes_\phi H$. Con ello, $\sigma^i = (g^i, (1, 1)^i) \Rightarrow o(\sigma) = mcm(o(g), o((1, 1))) = 2p$, y es claro que $o(\tau) = 2$. Finalmente, se da que

$$\sigma\tau = (g, (1, 1))(g, (1, 0)) = (g^2, (0, 1)) = (g\eta(g^{-1}), (0, 1)) = (g, (1, 0))(g^{-1}, (1, 1)) = \tau\sigma^{-1}$$

con lo que $G \cong D_{2p}$

Consideremos ahora $H \cong C_4$. Si $\phi \equiv 1_{Aut(N)}$, por 1.3.1, $G \cong C_{4p}$. En cambio, si $\phi \not\equiv 1_{Aut(N)}$, suponiendo $H = \langle h\rangle$, se tendrá $\phi(h) \neq 1_{Aut(N)}$. Tengamos en cuenta que, como antes, $Aut(N) \cong C_{p-1}$ y, por 3.2.3 existe un único $\eta \in Aut(N)$ de orden dos. Puede ser, además, que $4 \mid p-1$, y

que por tanto haya también en $Aut(N)$ dos elementos de orden 4, según nos dice 3.2.2, a los que podemos llamar $\zeta$ y $\zeta^{-1}$.

Cuando, $4 \nmid p-1$, como $o(h)=4$ y $o(\phi(h)) \mid o(h)$, necesariamente $o(\phi(h))=2$, y por tanto $\phi(h)=\eta$. Tomemos, en este caso, de $N \rtimes_\phi H$ los elementos $x=(g,h^2), t=(g,h^p)$. Como $\phi(h^2)=1_{Aut(N)}$, $x^n=(g^n,h^{2n})$, con lo que en particular $o(x)=mcm(o(h^2),o(g))=mcm(2,p)=2p$, $x^{2p}=1_G$ y $x^p=(g^p,h^{2p})=(1_N,h^{2p})$. Por otro lado, $\phi(h^p)=\eta$ tanto si $p\equiv 1(4)$ como si $p\equiv 3(4)$, por lo que $t^2=(g,h^p)(g,h^p)=(g\eta(g),h^{2p})=(1_N,h^{2p})$, y así $x^p=t^2$. Finalmente, operando tenemos

$$xt=(g,h^2)(g,h^p)=(g^2,h^{p+2})=(g\eta(g^{-1}),h^{p+2})=(g,h^p)(g^{-1},h^2)=tx^{-1}$$

de modo que $G\cong DC_p$.

Por último, si $4 \mid p-1$ debemos considerar una posibilidad adicional. Por 3.2.1, tenemos los mencionados elementos $\zeta,\zeta^{-1}\in Aut(N)$ de orden 4 con lo que también puede darse también que $\phi(h)=\zeta$ (el caso para $\zeta^{-1}$ es análogo por 1.2.2), lo que nos da un quinto posible grupo. En este caso, tomemos los elementos $x=(g,1_H), t=(g,h)$ de $N\rtimes_\phi H$. Por un lado, $o(x)=mcm(o(1_H),o(g))=p$, con lo que $x^p=1_N1$. Por otro, $t^2=(g,h)(g,h)=(g\zeta(g),h^2)$, luego $t^4=(g\zeta(g),h^2)(g\zeta(g),h^2)=(g\zeta(g)\eta(g\zeta(g)),h^4)=1_G$. Además, $t^{-1}=(\zeta^{-1}(g^{-1}),h^3)$, de modo que

$$\begin{aligned} txt^{-1}=(g,h)(g,1_H)(\zeta^{-1}(g^{-1}),h^3)=(g\zeta(g),h)(\zeta^{-1}(g^{-1}),h^3)= \\ (g\zeta(g)\zeta(\zeta^{-1}(g^{-1})),h^4)=(g\zeta(g)g^{-1},1_H)=(\zeta(g),1_H)\end{aligned}$$

y así $G\cong E_p$. Q.E.D.

Terminemos con este lema en el que se cifran los casos $3p$, $5p$, $7p$...

**Teorema 4.3.3.** *Sea $G$ un grupo de orden $pq$, con $p,q\in\mathbb{P}$ y $p<q$. Entonces $G$ es isomorfo a uno de los siguientes grupos*

- $C_{pq}$
- $C_q\rtimes C_p=\langle x,y|x^q=y^p=1,yxy^{-1}=x^{-1}\rangle$, *pero sólo cuando* $p\mid q-1$.

*Demostración.* Por el teorema de Cauchy sabemos que existen $g,h\in G$ de órdenes $q$ y $p$ respectivamente. Por el lema 3.3.2, como $o(\langle g\rangle)=q$ y $[G:\langle g\rangle]=p$, se da que $\langle g\rangle \triangleleft G$. Llamemos $N=\langle g\rangle$ y $H=\langle h\rangle$. Se da que $N\cap H=\{1_G\}$ porque los dos subgrupos tienen órdenes coprimos, y $o(N)o(H)=pq=o(G)$, con lo que por 3.3.4 $G=NH$. Por ello, en virtud de 1.2.1 existirá un homomorfismo $\phi: H\to Aut(N)$ tal que $G\cong N\rtimes_\phi H$.

Como $Aut(N)\cong Aut(C_q)\cong C_{q-1}$, como decíamos en 3.1.1 (no puede darse $q=2$ porque $p<q$), si $p\nmid q-1$, la imagen de $h$ por $\phi$ necesariamente deberá ser $1_{Aut(N)}$, pues $o(\phi(h))\mid o(h)$ y, como $o(h)$ es primo, o bien $o(\phi(h))=1$ o bien $o(\phi(h))=o(h)=p$ pero en este último caso tendríamos $o(\phi(h))=p\nmid q-1=o(Aut(N))$, lo cual contradice el teorema de Lagrange. Así, en este primer caso, sólo puede darse $\phi\equiv 1_{Aut(N)}$, que por 1.3.1 quiere decir que $G\cong N\rtimes_\phi H\cong N\times H\cong C_q\times C_p\cong C_{pq}$.

Ahora bien, cuando $p\mid q-1$, $\phi(h)$ puede ser cualquier elemento de orden $q-1$ en $Aut(N)$, es decir, cualquier generador. En particular, podemos tomar $\zeta: N\to N: g\mapsto g^2$. Como $q\neq 2$ se da $mcd(q,2)=1$, y por tanto $\langle g\rangle=\langle g^2\rangle$. Esto nos dice que $\zeta$ va a ser un automorfismo, y además este va a ser de orden $q-1$, porque por el teorema de Euler, $2^{\varphi(q)}\equiv 1(q)$, con lo que $\zeta^{q-1}=1_{Aut(N)}$ y no puede darse $o(\zeta)<q-1$, pues en tal caso no sería cierto que $\langle g\rangle=\langle g^2\rangle$, sino que el segundo sería un subgrupo propio del primero. Por ello, podemos afirmar $\phi(h)=\zeta$. Esta afirmación se hace sin pérdida de generalidad: si consideramos otro automorfismo $\delta: N\to N$

y su correspondiente homomorfismo $\psi : H \to Aut(N) : h \mapsto \delta$, como $\delta \in Aut(N) = \langle \zeta \rangle$, $\delta = \zeta^i, i \in \{1, ..., q-1\}$, basta tomar $\beta : H \to H : h \mapsto h^i$, tener en cuenta que $\psi = \phi \circ \beta$ (porque $\psi(h) = \delta = \zeta^i = \phi(h)^i = \phi(h^i) = \phi(\beta(h))$) y aplicar 1.2.2 para darse cuenta de que estos dos homomorfismos definen productos semidirectos isomorfos.

Para ver que este producto semidirecto cumple la descripción dada en el enunciado, tomemos elementos $x = (g, 1_H)$ e $y = (1_N, h)$ en $N \rtimes_\phi H$. Es claro que $o(x) = o(g) = q$ y $o(y) = o(h) = p$. Antes de concluir hay que señalar que, como ya hemos dicho, por el teorema de Euler $q \mid 2^{q-1}$, y por tanto la aplicación inversa de $\zeta$ será $\zeta^{-1} : N \to N : g \mapsto g^{2^{q-2}}$. Con ello concluimos:

$$yxy^{-1} = (1_N, h)(g, 1_H)(1_N, h^{-1}) = (g, h)(1_N, h^{-1}) = (\zeta^{-1}(g), 1_H) = (g^{2^{q-2}}, 1_H) = x^{-1}$$

Q.E.D.

# Capítulo 5

# Un problema singular: Grupos de orden $2k$

## 5.1. Presentación y motivación del problema

En las páginas siguientes resolveremos un problema distinto, aunque en la línea de lo que venimos haciendo: el de clasificar los grupos de orden $2k$ cuando estos tienen al menos un elemento $g$ de orden $k$. El interés por este problema se ha suscitado en el estudio de grupos de automorfismos de superficies de Klein con borde. En efecto, al intentar obtener los grupos de automorfismos de una de estas superficies con 2 componentes conexas en el borde, se plantean dos situaciones: o bien el tal grupo tiene orden impar, y entonces es cíclico, o bien es par, y entonces tiene un subgrupo cíclico de índice 2 (véase [3]). Por ello, para poder estudiar qué grupos aparecen se hace necesario clasificar los grupos de orden $2k$ que contengan un elemento de orden $k$. Aparentemente, y salvo un caso particular como veremos, este resultado no se conoce, y a obtenerlo hemos dedicado este capítulo.

Resolveremos el problema en dos casos: cuando $k$ sea impar y cuando $k$ sea par (que llegado el momento, por comodidad, lo llamaremos $2^m k$, para $k$ impar). En el caso para $k$ impar se pueden ubicar los subgrupos necesarios para dar un producto semidirecto. No será así en el caso en que $k$ es par, donde rápidamente encontramos dos familias de contraejemplos: la de algunos cíclicos y la de todos los dicíclicos.

Para salir del callejón introduciremos un caso muy concreto en el que la cuestión se reduce a un problema de cómputo: el del 2-grupo (tal y como la desarrolló Gorenstein en [6]). Apoyándonos en éste podremos, con algebraica cautela, generalizarlo al caso par.

## 5.2. Caso para el orden de $g$ impar

Comenzamos, como acordamos, por el caso en que el orden de $g$ es impar.

**Teorema 5.2.1.** *Sea $G$ un grupo de orden $2k$, con $k \in \mathbb{N}$ impar, y un elemento $g \in G$ de orden $k$. Entonces $\exists k_1, k_2 \in \mathbb{N} : k = k_1 k_2, mcd(k_1, k_2) = 1, G \cong C_{k_1} \times D_{k_2}$.*

*Demostración.* Como $[G : \langle g \rangle] = 2$, entonces $\langle g \rangle \triangleleft G$ en virtud de 3.3.2. Además, por el teorema de Cauchy, $\exists h \in G : h^2 = 1_G$ y, como $k$ es impar, $h \notin \langle g \rangle$. Llamemos, por comodidad $N = \langle g \rangle, H = \langle h \rangle$. De este modo, como $H \cap N = \{1_G\}$ y $HN = G$, por 1.2.1, $\exists \phi : H \to Aut(N) : G \cong N \rtimes_\phi H$.

Supongamos ahora que $k = p_1^{\alpha_1} ... p_r^{\alpha_r}, p_i \in \mathbb{P} \setminus \{2\}, \alpha_i \in \mathbb{N}, \forall i \in \{1, ..., n\}$, con los primos $p_i$ distintos entre sí, de forma que

$$N = \langle g \rangle \cong C_k \cong C_{p_1^{\alpha_1}} \times ... \times C_{p_r^{\alpha_r}}$$

y así, por 3.1.1 y 3.1.5, $Aut(N) \cong C_{p_1^{\alpha_1-1}(p_1-1)} \times ... \times C_{p_r^{\alpha_r-1}(p_r-1)}$. Denotemos por $g_i$ al generador de cada $C_{p_i^{\alpha_i}}$.

Dado $i \in \{1, ..., n\}$ arbitrario, puesto que $2 \mid (p_i - 1)$, en cada $C_{p_i^{\alpha_i-1}(p_i-1)}$ hay, por 3.2.3, un único elemento $\eta_i \in Aut(C_{p_i^{\alpha_i}})$ de orden 2. Nótese que éste elemento cumplirá $\eta_i(x) = x^{-1}, \forall x \in C_{p_i^{\alpha_i}}$, pues el automorfismo $x \mapsto x^{-1}$ es de orden dos.

Con todo ello, sabemos que $\phi(h)$ debe ser un elemento de orden divisor de dos en $Aut(N)$. Como en cada $C_{p_i^{\alpha_i}}$ hay un único elemento de orden dos, se tendrá que la proyección de $\phi(h)$ a $Aut(C_{p_i^{\alpha_i}})$ será, o bien $1_{Aut(N)}$, o bien $\eta_i$. Así, reordenando sin pérdida de generalidad, para cierto $0 \leq s \leq r$,

$$\begin{aligned} \phi : H &\longrightarrow Aut(N) \cong Aut(C_{p_1^{\alpha}{}_1}) \times ... \times Aut(C_{p_r^{\alpha}{}_r}) \\ h &\longmapsto (1_{Aut(C_{p_1^{\alpha_1}})}, ..., 1_{Aut(C_{p_s^{\alpha_s}})}, \eta_{s+1}, ..., \eta_r) \end{aligned}$$

Tomemos así los elementos de $N \times H$:

$$\begin{aligned} x &= ((g_1, ..., g_s, 1, ..., 1), 1_H). \\ \sigma &= ((1, ..., 1, g_{s+1}, ..., g_r), 1_H). \\ \tau &= (1_N, h). \end{aligned}$$

De modo que, tomando $k_1 = p_1^{\alpha_1}...p_s^{\alpha_s}, k_2 = p_{s+1}^{\alpha_{s+1}}...p_r^{\alpha_r}$ se verifica:

$$\begin{aligned} o(x) &= o((g_1, ..., g_s, 1, ..., 1)) = mcm\{o(g_i) : 1 \leq i \leq s\} = k_1. \\ o(\sigma) &= o((1, ..., 1, g_{s+1}, ..., g_r)) = mcm\{o(g_i) : s+1 \leq i \leq r\} = k_2. \\ o(\tau) &= 2 \end{aligned}$$

Por distinción de órdenes es claro que $a \notin \langle b \rangle, \forall a, b \in \{x, \sigma, \tau\}$, de modo que, como $o(G) = 2k = 2k_1k_2 = o(\tau)o(x)o(\sigma)$, se tiene, por 3.3.4 $G = \langle x \rangle \langle \sigma \rangle \langle \tau \rangle = \langle x, \sigma, \tau \rangle$. Sabemos entonces que cada elemento $g \in G$ admite una única representación

$$g = x^i \sigma^j \tau^\delta, i \in \{0, 1, ..., k_1 - 1\}, j \in \{0, 1, ..., k_2 - 1\}, \delta \in \{0, 1\}$$

pues cada pareja de $\{\langle x \rangle, \langle \sigma \rangle, \langle \tau \rangle\}$ tiene intersección $\{1_G\}$. Comprobamos también:

$x\sigma = \sigma x$

$$\begin{aligned} x\sigma &= ((g_1, ..., g_s, 1, ..., 1), 1_H)((1, ..., 1, g_{s+1}, ..., g_r), 1_H) = ((g_1, ..., g_r), 1_H) \\ \sigma x &= ((1, ..., 1, g_{s+1}, ..., g_r), 1_H)((g_1, ..., g_s, 1, ..., 1), 1_H) = ((g_1, ..., g_r), 1_H) \end{aligned}$$

$x\tau = \tau x$

$$\begin{aligned} x\tau &= ((g_1, ..., g_s, 1, ..., 1), 1_H)(1_N, h) = ((g_1, ..., g_s, 1, ..., 1), h) \\ \tau x &= (1_N, h)((g_1, ..., g_s, 1, ..., 1), 1_H) = ((g_1, ..., g_s, 1, ..., 1), h) \end{aligned}$$

$\sigma\tau = \tau\sigma^{-1}$

$$\begin{aligned} \sigma^{-1} &= ((1, ..., 1, g_{s+1}^{-1}, ..., g_r^{-1}), 1_H) \\ \sigma\tau &= ((1, ..., 1, g_{s+1}, ..., g_r), 1_H)(1_N, h) = ((1, ..., 1, g_{s+1}, ..., g_r), h) \\ \tau\sigma^{-1} &= (1_N, h)((1, ..., 1, g_{s+1}^{-1}, ..., g_r^{-1}), 1_H) = ((1, ..., 1, g_{s+1}, ..., g_r), h) \end{aligned}$$

Así, denotando $C_{k_1} = \langle a | a^{k_1} = 1 \rangle$ y $D_{k_2} = \langle b, c | b^{k_2} = c^2 = 1, cbc^{-1} = b^{-1} \rangle$ podemos definir la función

$$\begin{aligned} \gamma : G &\longrightarrow C_{k_1} \times D_{k_2} \\ g = x^i \sigma^j \tau^\delta &\longmapsto (a^i, b^j c^\delta) \end{aligned}$$

Comprobemos que es isomorfismo. Es inyectiva por la unicidad de representación de $g \in G$. Es sobreyectiva ya que dado $(a^i, b^j c^\delta) \in C_{k_1} \times D_{k_2}$ podemos tomar $x^i \sigma^j \tau^\delta \in G$ cuya imagen es el primer elemento. Finalmente, para demostrar que es homomorfismo tomemos elementos $g_1 = x^{i_1} \sigma^{j_1} \tau^{\delta_1}$ y $g_2 = x^{i_2} \sigma^{j_2} \tau^{\delta_2}$. Teniendo en cuenta las propiedades expuestas anteriormente acerca de cómo conmutan los elementos $x$, $\sigma$ y $\tau$, podemos distinguir los siguientes casos:

Cuando $\delta_1 = 0$:

$$\begin{aligned} f(g_1 g_2) &= f(x^{i_1} \sigma^{j_1} \tau^{\delta_1} x^{i_2} \sigma^{j_2} \tau^{\delta_2}) = f(x^{i_1+i_2} \sigma^{j_1+j_2} \tau^{\delta_2}) \\ &= (a^{i_1+i_2}, b^{j_1+j_2} c^{\delta_2}) = (a^{i_1}, b^{j_1})(a^{i_2}, b^{j_2} c^{\delta_2}) \\ &= f(x^{i_1} \sigma^{j_1}) f(x^{i_2} \sigma^{j_2} \tau^{\delta_2}) = f(g_1) f(g_2) \end{aligned}$$

Cuando $\delta_1 = 1$:

$$\begin{aligned} f(g_1 g_2) &= f(x^{i_1} \sigma^{j_1} \tau^{\delta_1} x^{i_2} \sigma^{j_2} \tau^{\delta_2}) = f(x^{i_1+i_2} \sigma^{j_1} \tau \sigma^{j_2} \tau \tau^{\delta_2 - 1}) \\ &= f(x^{i_1+i_2} \sigma^{j_1} (\tau \sigma \tau)^{j_2} \tau^{\delta_2 - 1}) = f(x^{i_1+i_2} \sigma^{j_1} \sigma^{-j_2} \tau^{\delta_2 - 1}) \\ &= f(x^{i_1+i_2} \sigma^{j_1 - j_2} \tau^{\delta_2 - 1}) = (a^{i_1+i_2}, b^{j_1 - j_2} c^{\delta_2 - 1}) \\ &= (a^{i_1+i_2}, b^{j_1} (cbc)^{j_2} c^{\delta_2 - 1}) = (a^{i_1+i_2}, b^{j_1} (cb^{j_2} c) c^{\delta_2 - 1}) \\ &= (a^{i_1+i_2}, b^{j_1} c b^{j_2} c^{\delta_2}) = (a^{i_1}, b^{j_1} c)(a^{i_2}, b^{j_2} c^{\delta_2}) \\ &= f(g_1) f(g_2) \end{aligned}$$

Lo que nos da el resultado deseado.

Q.E.D.

## 5.3. Caso del 2-grupo

El procedimiento anterior no puede aplicarse, sin embargo, cuando el orden de $g$ es par. Sin ir más lejos, si tomamos un grupo cíclico de orden par, por 3.2.3, éste tendrá sólo un elemento de orden dos, que por la misma razón se encontrará dentro de $\langle g \rangle$, lo que no nos permite encontrar el $h \in G \setminus \langle g \rangle$ anterior. Podríamos pensar ingenuamente que ésto sólo se puede dar en los casos abelianos (y por poco es así) y, teniendo éstos claros por el teorema de clasificación de los grupos finitos abelianos, seguir con ello dejándolos al margen. Tampoco esta salida es posible, y la evidencia la da el ejemplo 2.2.1, el grupo cuaternión, $Q$, que teniendo orden 8 y elementos de orden 4 no tiene ningún elemento de orden 2 fuera de los subgrupos de orden 4. En realidad no será así tampoco en ninguno de los dicíclicos, ni en el producto directo de un cíclico de orden impar por cualquiera de los hasta ahora mencionados.

Partiremos entonces de una situación más concreta: cuando $G$ es un 2-grupo. El siguiente lema ha sido extraído de [6], y puede consultarse para más información.

**Lema 5.3.1.** *Llamemos $N = \langle g \rangle$. Sea $G$ un grupo no abeliano de orden $2^{n+1}$ con un elemento $g \in G$ de orden $2^n$, para $n \in \mathbb{N}$ y $n \geq 3$. Entonces $G$ es isomorfo a uno de los grupos siguientes*

- $D_{2^n} = \langle x, y | x^{2^n} = y^2 = 1, yxy^{-1} = x^{-1} \rangle$

- $DC_{2^{n-1}} = \langle x, y | x^{2^{n-1}} = y^2 = z, z^2 = 1, yxy^{-1} = x^{-1} \rangle$
- $QA_n = \langle x, y | x^{2^n} = y^2 = 1, yxy^{-1} = x^{1+2^{n-1}} \rangle$
- $QD_n = \langle x, y | x^{2^n} = y^2 = 1, yxy^{-1} = x^{-1+2^{n-1}} \rangle$.

*Demostración.* Como $G$ no es abeliano, existe $h \in G \setminus N$ que no conmuta con todos los elementos de $N$. En particular, no puede conmutar con $g$, pues en tal caso conmutaría con todos los de $N$. Así, la aplicación $\varphi : N \to N : x \mapsto hxh^{-1}$ es un automorfismo de $N$ distinto de la identidad, porque $hgh^{-1} \neq g$. Por 3.3.3, sabemos que $o(\varphi) \mid [G : N] = 2$, y como no tiene orden uno porque no es la identidad, necesariamente $o(\varphi) = 2$. Sabemos también que $G = \langle g, h \rangle$, porque $\langle g \rangle \subsetneq \langle g, h \rangle$ con lo que $[G : \langle g, h \rangle] < [G : \langle g \rangle]$, y como $[G : \langle g \rangle] = 2$ tendremos $[G : \langle g, h \rangle] = 1$, y por tanto $G = \langle g, h \rangle$. Además, $o(\varphi) = 2$, luego $\varphi^2 = Id_N$, y así

$$\varphi^2(g) = g \Rightarrow h^2 g h^{-2} = g \Rightarrow h^2 g = g h^2 \Rightarrow h^2 \in Z(G)$$

Continuando, como $Aut(N) \cong Aut(C_{2^n}) \cong C_2 \times C_{2^{n-2}}$, y sabiendo que $\varphi$ es de orden dos, las posibilidades que tenemos son:

1. $\varphi(g) = g^{1+2^{n-1}}$
2. $\varphi(g) = g^{-1}$
3. $\varphi(g) = g^{-1+2^{n-1}}$

Cabe señalar que cualquier elemento de $G$ se puede escribir de la forma $g^i h^j, i \in \{0, ..., 2^n - 1\}, j \in \{0, 1\}$, ya que éstos cubren los $2^{n+1}$ elementos de $G$ y son distintos entre sí (de lo contrario entontraríamos un absurdo en el que $g$ y $h$ conmutan). Con esto ya podemos empezar a determinar los grupos posibles. Estudiemos estos casos por separado.

1) Cuando $\varphi(g) = g^{1+2^{n-1}}$, tenemos que:

$$hg^2h^{-1} = hgh^{-1}hgh^{-1} = (hgh^{-1})^2 = (g^{1+2^{n-1}})^2 = g^{2+2^n} = g^2 \Rightarrow hg^2 = g^2h$$

Así, $g^2$ conmuta con $g$ y $h$, luego $g^2 \in Z(G)$. Veamos que, además, $Z(G) = \langle g^2 \rangle$, viendo que no puede ser mayor al no poder haber ningún otro elemento en el centro. Ya sabemos que $h \notin Z(G)$. Si en $Z(G)$ hubiese alguna potencia de $g$ de exponente impar, por estar $g^2$, estaría también $g$, lo cual no es cierto. Si en $Z(G)$ hubiese un elemento del tipo $g^{2t}h$, al estar $g^{2t}$ estaría también $h$, lo cual no es cierto. Si lo hubiese de la forma $g^{2t+1}h$, por estar $g^2$ también estaría $gh$, pero esto es absurdo, pues si es así se da $g(gh) = (gh)g \Rightarrow gh = hg$.

Añadiendo que, como dijimos, $h^2 \in Z(G)$, existirá un $a \in \mathbb{N}$ tal que $h^2 = (g^2)^a = g^{2a}$. Tomemos entonces $c \in \mathbb{N}$ que satisfaga

$$a + c(1 + 2^{n-2}) \equiv 0(2^{n-1})$$

lo cual es legítimo puesto que $n > 2$. Tomando entonces $y = g^c h$ tenemos

$$\begin{aligned} y^2 = (g^c h)^2 = g^c h g^c h = g^c h g^c h^{-1} hh = g^c (g^c)^{1+2^{n-1}} h^2 \\ = g^{c(2+2^{n-1})} g^{2a} = g^{2(a+c(1+2^{n-2}))} = g^{2(2^{n-1})t} = g^{2^n t} = 1_G \end{aligned}$$

y además

$$ygy^{-1} = (g^c h) g (h^{-1} g^{-c}) = g^c (hgh^{-1}) g^{-c} = g^c g^{1+2^{n-1}} g^{-c} = g^{1+2^{n-1}}$$

y por lo tanto

$$G \cong QA_n = \langle g, y | g^{2^n} = y^2 = 1, ygy^{-1} = g^{1+2^{n-1}} \rangle$$

2) Cuando $\varphi(g) = g^{-1}$, es fácil comprobar que $g^{2^{n-1}}$ conmuta con $h$

$$\begin{aligned} hg^{2^{n-1}}h^{-1} &= (hgh^{-1})^{2^{n-1}} = (g^{-1})^{2^{n-1}} = g^{-(2^{n-1})} \\ &= g^{2^n-(2^n-1)} = g^{2^{n-1}(2-1)} = g^{2^{n-1}} \\ &\Rightarrow hg^{2^{n-1}} = g^{2^{n-1}}h \end{aligned}$$

Comprobemos que, además, se tendrá $Z(G) = \langle g^{2^{n-1}} \rangle$. Veamos que no puede ser mayor viendo que ningún otro elemento está en el centro. De antemano contamos con que $h \notin Z(G)$. Si $g^t \in Z(G), t \in \{1, ..., 2^n - 1\}$, entonces

$$hg^th^{-1} = (hgh^{-1})^t = (g^{-1})^t = g^{-t} \Rightarrow hg^t = g^{-t}h \Rightarrow g^t = g^{-t} \Rightarrow g^{2t} = 1_G \Rightarrow t = 2^{n-1}$$

con lo que se trata del elemento que ya sabíamos que estaba dentro. Si $g^th \in Z(G), t \in \{1, ..., 2^n - 1\}$ entonces

$$h(g^th)h^{-1} = hg^th^{-1}h = g^{-t}h \Rightarrow g^th = g^{-t}h \Rightarrow g^{2t} = 1_G \Rightarrow t = 2^{n-1}$$

pero como además $g^{2n-1} \in Z(G)$, esto significaría que $h \in Z(G)$, que no es así.

Ahora, como $h^2 \in Z(G)$, existe $a \in \mathbb{N}$ tal que $h^2 = (g^{2^{n-1}})^a = g^{2^{n-1}a}$.

Si $2 \mid a$, entonces $a = 2a'$, luego $h^2 = g^{2^n a'} = 1_G$, y por tanto

$$G \cong D_{2^n} = \langle g, h | g^{2^n} = h^2 = 1, hgh^{-1} = g^{-1} \rangle$$

Si $2 \nmid a$, entonces $a = 2a' + 1$, luego $h^2 = g^{2^n a' + 2^{n-1}} = g^{2^{n-1}}$, y así

$$G \cong DC_{2^{n-1}} = \langle g, h | g^{2^{n-1}} = h^2 = m, m^2 = 1, hgh^{-1} = g^{-1} \rangle$$

3) Cuando $\varphi(g) = g^{-1+2^{n-1}}$, de nuevo $g^{2^{n-1}}$ conmuta con $h$:

$$\begin{aligned} hg^{2^{n-1}}h^{-1} &= (hgh^{-1})^{2^{n-1}} = (g^{-1+2^{n-1}})^{2^{n-1}} = g^{-2^{n-1}+2^{2n-2}} \\ &= g^{-2^{n-1}}g^{2^{2n-2}} = g^{2^n-2^{n-1}}g^{2^n 2^{n-2}} = g^{2^{n-1}(2-1)}(g^{2^n})^{2^{n-2}} = g^{2^{n-1}} \end{aligned}$$

Veamos que esta vez $Z(G) = \langle g^{2^{n-1}} \rangle$, viendo de nuevo que no hay en el centro ningún otro elemento. Como ya hemos dicho, $h \notin Z(G)$. Si $g^{2t} \in Z(G), t \in \{1, ..., 2^n - 1\}$,

$$hg^{2t}h^{-1} = (hgh^{-1})^{2t} = (g^{-1+2^{n-1}})^{2t} = g^{-2t} \Rightarrow g^{4t} = 1_G \Rightarrow 2^{n-2} \mid t$$

de modo que $t$ estará en $\{2^{n-2}, 2^{n-1}, 2^{n-2}3\}$. En el primer y segundo casos nos da que $g^{2t}$ es $g^{2^{n-1}}$ y $1_G$ respectivamente, con lo que sólo debemos buscar un absurdo en el tercer caso. Si $g^{2^{n-1}3} \in Z(G)$ también $g^3 \in Z(G)$. Con ello

$$hg^3h^{-1} = (hgh^{-1})^3 = (g^{-1+2^{n-1}})^3 = g^{3\cdot 2^{n-1}-3} = g^{2^{n-1}-3} \Rightarrow g^3 = g^{2^{n-1}-3} \Rightarrow g^{2^{n-1}-6} = 1_G,$$

lo cual es absurdo. Por otro lado, si $g^{2t+1} \in Z(G), t \in \{1, ..., 2^n - 1\}$ se dará:

$$\begin{aligned} &hg^{2t+1}h^{-1} = (hgh^{-1})^{2t+1} = (g^{-1+2^{n-1}})^{2t+1} = g^{2^{n-1}-2t-1} \\ &\Rightarrow g^{2t+1} = g^{2^{n-1}-2t-1} \Rightarrow g^{2^{n-1}-4t-2} = 1_G \Rightarrow g^{2(2^{n-2}-2t-1)} = 1_G \\ &\Rightarrow 2^{n-1} \mid 2^{n-2} - 2t - 1 \end{aligned}$$

lo cual es ridículo porque el primero es potencia de dos y el segundo impar. De nuevo, para elementos de la forma $g^{2t}h$ o $g^{2t+1}h$ obtendremos los mismos absurdos. Como $h^2 \in Z(G)$, existe $a \in \mathbb{N}$ tal que $h^2 = (g^{2^{n-1}})^a = g^{2^{n-1}a}$.

Si $2 \mid a$, entonces $a = 2a'$, luego $h^2 = g^{2^n a'} = 1_G$, y con ello

$$G \cong QD_n = \langle g, h | g^{2^n} = h^2 = 1, hgh^{-1} = g^{-1+2^{n-1}} \rangle$$

Si $2 \nmid a$, entonces $a = 2a' + 1$, luego $h^2 = g^{2^n a' + 2^{n-1}} = g^{2^{n-1}} \Rightarrow G \cong \langle g, h | g^{2^{n-1}} = h^2 = m, m^2 = 1, hgh^{-1} = g^{-1+2^{n-1}} \rangle$. Claro que en este caso podemos encontrar una presentación mejor. Tomando $y = gh$ se tiene

$$y^2 = (gh)^2 = ghgh = g(hgh^{-1})hh = gg^{-1+2^{n-1}}h^2 = g^{2^{n-1}}g^{2^{n-1}} = g^{2^n} = 1_G$$

y

$$ygy^{-1} = (gh)g(h^{-1}g^{-1}) = g(hgh^{-1})g^{-1} = gg^{1+2^{n-1}}g^{-1} = g^{1+2^{n-1}}$$

y así, de nuevo,

$$G \cong QD_n = \langle g, y | g^{2^n} = y^2 = 1, ygy^{-1} = g^{-1+2^{n-1}} \rangle$$

Q.E.D.

## 5.4. Caso para orden de $g$ par

Teniendo pues los posibles 2-grupos con un elemento $g$ como el descrito, vamos a tratar de descomponer nuestro grupo $G$ lo suficiente para que, aplicando 5.3.1, sólo nos quede resolver una serie de cuentas.

**Teorema 5.4.1.** *Sea $G$ un grupo no abeliano de orden $2^{n+1}k$, con $n, k \in \mathbb{N}$, $k$ impar, tal que tiene un elemento $g \in G$ de orden $2^n k$. Entones existen $k_1, k_2 \in \mathbb{N}$ con $k = k_1 k_2$ y $mcd(k_1, k_2) = 1$ de forma que $G$ es isomorfo a $C_{k_1} \times K$, donde $K$ es uno de los siguientes grupos*

- $C_{2^n} \times D_{k_2}$
- $C_{k_2} \rtimes C_{2^{n+1}} = \langle z, w | z^{k_2} = w^{2^{n+1}} = 1, wzw^{-1} = z^{-1} \rangle$
- $D_{2^n k_2} = \langle v, w | v^{2^n k_2} = w^2 = 1, vvw^{-1} = v^{-1} \rangle$
- $DC_{2^{n-1}k_2} = \langle v, w | v^{2^n k_2} = 1, v^{2^{n-1}k_2} = w^2, vvw^{-1} = v^{-1} \rangle$
- $\langle x, z, w | x^{2^n} = z^{k_2} = w^2 = 1, wxw^{-1} = x^{1+2^{n-1}}, wzw^{-1} = z^{-1}, xz = zx \rangle$
- $\langle x, z, w | x^{2^n} = z^{k_2} = w^2 = 1, wxw^{-1} = x^{-1+2^{n-1}}, wzw^{-1} = z^{-1}, xz = zx \rangle$.

*Además, cuando $n = 1$ sólo puede serlo a dos primeros casos y cuando $n = 2$ a los cuatro primeros casos .*

*Demostración.* Llamemos $N = \langle g \rangle$. Por el teorema fundamental de la aritmética, $k = p_1^{\alpha_1} ... p_r^{\alpha_r}$, con $p_i \in \mathbb{P} \setminus \{2\}, \alpha_i \in \mathbb{N}, \forall i \in \{1, ..., r\}$ y los primos $p_i$ distintos entre sí. Como $G$ es no abeliano, necesariamente existe un $h \in G$ tal que $gh \neq hg$. Como $\langle g \rangle \subsetneq \langle g, h \rangle$ y $[G : \langle g \rangle] = 2$, necesariamente $G = \langle g, h \rangle$.

Tomando entonces el automorfismo $\varphi : N \to N : g \mapsto hgh^{-1}$ tenemos, por 3.3.3 y teniendo en cuenta que $\varphi$ no es la identidad porque no conmutan $g$ y $h$, que $o(\varphi) = 2$.

Considerando $\langle g \rangle \cong C_k \cong C_{2^n} \times C_{p_1^{\alpha_1}} \times ... \times C_{p_r^{\alpha_r}}$ tendremos que, por 3.1.1, $\varphi$ será en cada $C_{p_i^{\alpha_i}}$ la identidad o la aplicación $\lambda \mapsto \lambda^{-1}$ para cada elemento $\lambda$. Digamos que en $C_{p_1^{\alpha_1}}, ..., C_{p_s^{\alpha_s}}$ es la identidad y en $C_{p_{s+1}^{\alpha_{s+1}}}, ..., C_{p_r^{\alpha_r}}$ es la otra aplicación, para cierto $0 \leq s \leq r$. Llamemos también, $k_1 = p_1^{\alpha_1} ... p_s^{\alpha_s}$ y $k_2 = p_{s+1}^{\alpha_{s+1}} ... p_r^{\alpha_r}$, de tal modo que $mcd(k_1, k_2) = 1$ y $k = k_1 k_2$.

Teniendo en cuenta que $\langle g\rangle \cong C_{2^n} \times C_{k_1} \times C_{k_2}$, podemos tomar los elementos $x, y, z \in \langle g\rangle$ que generan cada $C_{2^n}$, $C_{k_1}$ y $C_{k_2}$ respectivamente, que conmutan entre sí, y cumplen $g = xyz$. De esta forma sabemos $\varphi(y) = y$ y $\varphi(z) = z^{-1}$. En breve nos preguntaremos por $\varphi(x)$.

Veamos el orden de $h$. Como, por el teorema de Lagrange, $o(h) \mid o(G)$, $o(h) = 2^m t, t \mid k, 0 < m \leq n{+}1$. Si consideramos $h^t$, por ser $t$ impar, $\varphi = \varphi^t$, y $o(h^t) = 2^m$. También se dará $G = \langle g, h^t\rangle$, porque como $h^t$ y $z$ no conmutan $h^t \notin \langle g\rangle$, que es abelinano, de modo que $\langle g\rangle \subsetneq \langle g, h^t\rangle$. Así, podemos sustituir el $h$ que habíamos tomado por $h^t$, de manera que se sigan cumpliendo todas las hipótesis requeridas, y suponer sin pérdida de generalidad que $h$ es de orden $2^m$.

Bajo la certeza de que $mcd(o(y), o(x)) = mcd(o(y), o(z)) = mcd(o(y), o(h)) = 1$ somos conscientes de que $\langle y\rangle \cap \langle x, z, h\rangle = \{1_G\}$, y por 3.3.5 se da $G \cong \langle y\rangle \times \langle x, z, h\rangle$. Sólo nos queda probar que $K = \langle x, z, h\rangle$ es uno de los señalados en el enunciado.

Sabemos que $h \notin \langle x, z\rangle$ porque $h \notin \langle g\rangle$. Al ser $[K : \langle x, z\rangle] = 2$, por 3.3.2, $\langle x, z\rangle \triangleleft K$. Llamaremos por ello en lo restante $\varphi$ a la restricción de $\varphi$ a $K$, es decir a la aplicación $\varphi : K \to K : \lambda \mapsto h\lambda h^{-1}$. Por 3.3.3, $o(\varphi) \mid 2$, y como $h$ y $z$ no conmutan, $o(\varphi) = 2$, al igual que en su caso general. Es cierto que $\varphi(z) = z^{-1}$, pero para $x$ tenemos varias posibilidades: $\varphi(x) = x$, $\varphi(x) = x^{-1}$, $\varphi(x) = x^{1+2^{n-1}}$ o $\varphi(x) = x^{-1+2^{n-1}}$, siendo posibles las dos últimas sólo cuando $n \geq 3$ y las tres últimas cuando $n \geq 2$.

Así pues, $o(x) = 2^n$ y $o(h) = 2^m$, con $h \notin \langle x\rangle$, de forma que $o(\langle x, h\rangle) = 2^{n+1}$. Miremos ahora las distintas opciones de $\varphi(x)$ para obtener los distintos grupos $\langle x, h\rangle$.

En el caso en que $\varphi(x) = x$, tenemos que $\langle x, h\rangle$ es un grupo de orden $2^{n+1}$ abeliano con un elemento de orden $2^n$. Por tanto, atendiendo al teorema de clasificación de los grupos abelianos finitos, $\langle x, h\rangle \cong C_{2^n} \times C_2$ o $\langle x, h\rangle \cong C_{2^{n+1}}$. En el primero de los casos, podemos suponer que $x = (a, 1_{C_2})$, donde $C_{2^n} = \langle a\rangle$ y $C_2 = \langle b\rangle$, pues éste es de orden $2^n$. Del mismo modo, $h$ no puede ser de la forma $(a^i, 1_{C_2})$, pues en tal caso se daría $h \in \langle x\rangle$, de modo que podemos tomar $h = (1_{C_{2^n}}, b)$ (si $h = (a^i, b)$ bastaría trazar un isomorfismo que fijase $x$ y mandase $h$ a $hx^{-i}$). Por tanto, aplicando 3.3.5 sobre el generador $x$, tenemos el primer grupo del enunciado. Si se da el segundo caso y $\langle x, h\rangle$ es isomorfo a un grupo cíclico, (digamos que es generado por $a$), entonces $\langle x, z, h\rangle = \langle z, a\rangle$, donde naturalmente $a^2$ conmuta con $z$, luego es necesario que $a$ no lo haga, y así tenemos el segundo grupo del enunciado.

Para los demas casos, sabemos que $\langle x, h\rangle$ no es abeliano y es de orden $2^{n+1}$. Supondremos ahora que $n \geq 3$, ya que todas las posibilidades para $n = 1$ ya las hemos abordado, y haremos una consideración final del caso en que $n = 2$. Aplicando 5.3.1, y dependiendo de la elección de $\varphi(x)$, tendremos que $\langle x, h\rangle$ es isomorfo a

$$QA_n = \langle x, w | x^{2^n} = w^2 = 1, wxw^{-1} = x^{1+2^{n-1}}\rangle \tag{5.1}$$

$$D_{2^n} = \langle x, w | x^{2^n} = w^2 = 1, wxw^{-1} = x^{-1}\rangle \tag{5.2}$$

$$Q_n = \langle x, w | x^{2^n} = 1, x^{2^{n-1}} = w^2, wxw^{-1} = x^{-1}\rangle \tag{5.3}$$

$$QD_n = \langle x, w | x^{2^n} = w^2 = 1, wxw^{-1} = x^{-1+2^{n-1}}\rangle, \tag{5.4}$$

donde el caso (5.1) se da cuando $\varphi(x) = x^{1+2^{n-1}}$, el caso (5.4) cuando $\varphi(x) = x^{-1+2^{n-1}}$, y los casos (5.2) y (5.3) cuando $\varphi(x) = x^{-1}$.

En cada caso podemos considerar que el elemento $x$ de la descripción de dichos grupos coincide con el elemento $x$ hasta aquí utilizado, y que por tanto va a conmutar con $z$. Sin embargo, no en todos los casos $h$ va a cumplir el papel de $w$, y por tanto no tendría por qué cumplirse que $wzw^{-1} = z^{-1} = \varphi(z)$. Sin embargo, sí va a ser así. Remitiéndonos a la demostración de 5.3.1 vemos qué sucede en cada grupo.

Si se da (5.1), $w = x^c h$, de forma que

$$wzw^{-1} = (x^c h)z(h^{-1}x^{-c}) = x^c z^{-1} x^{-c} = z^{-1},$$

luego $G = \langle x, z, w | x^{2^n} = z^{k_2} = w^2 = 1, wxw^{-1} = x^{1+2^{n-1}}, wzw^{-1} = z^{-1}, xz = zx \rangle$.

Si se da (5.4), $w = h$, de modo que $\varphi(z) = wzw^{-1}$, o $w = gh$, lo que nos da el mismo resultado porque $x$ conmuta con $z$. Por tanto, $G = \langle x, z, w | x^{2^n} = z^{k_2} = w^2 = 1, wxw^{-1} = x^{-1+2^{n-1}}, wzw^{-1} = z^{-1}, xz = zx \rangle$.

Si se da (5.2), $w = h$, y con esto tenemos, porque $x$ y $z$ conmutan, tomando $v = xz$,

$$wvw^{-1} = w(xz)w^{-1} = (wxw^{-1})(wzw^{-1}) = x^{-1}z^{-1} = z^{-1}x^{-1} = v^{-1},$$

y por tanto, $G = \langle v, w | v^{2^n k_2} = w^2 = 1, wvw^{-1} = v^{-1} \rangle$.

Si se da (5.3), $w = h$, llamando $v = xz$, $G = \langle v, w | v^{2^{n-1} k_2} = w^2 = m, m^2 = 1, wvw^{-1} = v^{-1} \rangle$.

Hablemos por último del caso en que $n = 2$. Por 3.1.2, como $o(\varphi) = 2$, puede darse que $\varphi(x) = x$ o que $\varphi(x) = x^{-1}$. El primero de los casos ya lo hemos analizado antes. Respecto al segundo, sabremos que $\langle x, h \rangle$ será un grupo no abeliano de orden 8, con un elemento de orden 4. Por lo tanto tendremos dos posibilidades, o bien $\langle x, h \rangle \cong D_4$, o bien $\langle x, h \rangle \cong Q$, el grupo cuaternión. Claro que éste último es el caso particular $DC_2$. A partir de aquí sólo es necesario seguir lo dicho de los casos (5.2) y (5.3) en el caso en que $n \geq 3$, antes señalado, para obtener de nuevo el tercer y cuarto grupo del enunciado. Q.E.D.

# Apéndice: Conclusión

## Una breve historia del problema

Como ya hemos insinuado, el problema de buscar una lista completa e irredundante de grupos es un problema de más de siglo y medio. El pistoletazo de salida lo dió Cayley entre 1854 y 1859, determinando los grupos cíclicos y los de orden 4, 6 y 8. Le siguió Netto en 1882 con los grupos de orden $p^2$ y $pq$ (donde se engloba $2p$). Kempe en 1886 determinó los de orden 8 (coincidiendo con el listado de Cayley) y 12. Sin embargo se equivocó, y los grupos de orden 12 fueron correctamente descritos por Cayley en 1889.

Los grupos de orden $p^3$ fueron descubiertos por separado en 1893 por Cole y Glover, Hölder y Young, logrando además los tres primeros también los órdenes $p^2q$ y $pqr$ (donde se engloba $4p$). No obstante, Hölder tuvo que rectificar en 1895 porque se equivocó en $p^2q$.

Más adelante, estando próxima la entrada en el tercer milenio, Besche, Eick y O'Brien determinaron todos los grupos de orden menor o igual que 2000, salvo los de 1024, haciendo uso de métodos computacionales. Esta lista está perfectamente disponible y manejable en la biblioteca digital GAP. Para más interés, la historia completa de la clasificación por orden puede encontrarse en [2].

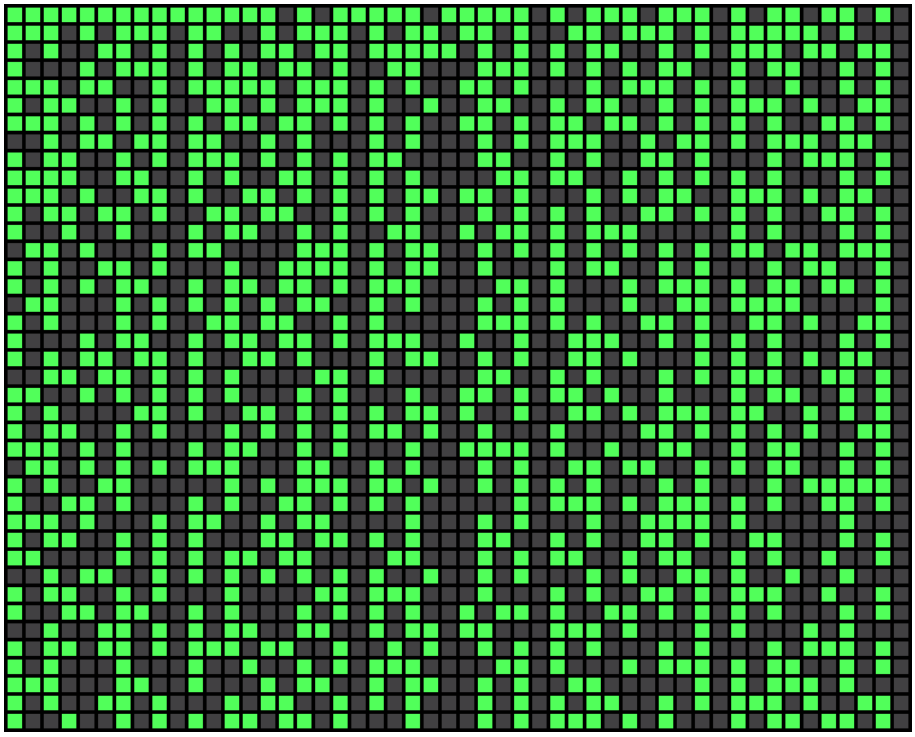
## Visualización de resultados

Después de cuarenta páginas es natural preguntarse cuántos grupos hemos determinado en este proceso. Vamos a ver qué resultado dan nuestros teoremas sobre los grupos de orden menor o igual que 2000, viendo qué parte de la lista de [2] hemos cubierto.

¿Cuántos de éstos hemos clasificado? Preguntado así la respuesta es decepcionante: de los 49.910.529.484 sólo hemos tratado con 1.600, un 0,0000032 % de los grupos de dicha lista. La cosa por supuesto tiene trampa. Lo cierto es que 49.487.365.422 de los grupos de orden menor o igual que 2000 son de orden $1024 = 2^{10}$, lo que representa un 99,152 % de ellos.

El 0,848 % restante también está disputado: hay 408.641.062 grupos de orden $1536 = 2^9 3$ y 10.494.213 de orden $512 = 2^9$. También se van más de un millón de grupos en $768 = 2^8 3$, $1280 = 2^8 5$ y $1792 = 2^8 7$. Éstos mencionados son el 0,846 %, con lo que de tener algo que decir será en ese escaso 0.002 % restante.

Si queremos ver algo en claro tenemos entonces que preguntarnos, viendo también la orientación y la forma de abordar los grupos que ha tenido este texto, de cuáles de los órdenes hasta 2000 hemos dado todas los posibles grupos a los que uno de dicho orden puede ser isomorfo. El resultado es en este caso más halagador. Si miramos la lista de naturales los primeros que no alcanzamos son 16, 18, 24, 30, 32, 36, 40... no muchos y alejados entre sí. De los 2000 primeros órdenes hemos clasificado 980, un 49 %, y hemos dejado en el tintero 1020. También se puede decir que de esos 1020, 302 son de orden $pqr$, que con ayuda del bagaje técnico a nuestras espaldas no habría sido difícil de determinar.



*En la siguiente imagen se muestran 2000 celdas, numeradas en orden de escritura y coloreadas de verde si ese concreto orden ha sido determinado en el trabajo.*

# Apéndice: Resultados fundamentales

Adjuntamos al lector algunos de los resultados más relevantes de los ámbitos de la matemática que en este trabajo manejamos, suponiéndo que éste los conoce, pero estimando necesario especificar la versión exacta de éstos que manejamos en el texto.

## Función Phi de Euler

**Definición 1.** *Llamamos función phi de Euler a la función* $\varphi : \mathbb{N} \to \mathbb{N}$ *que asocia a cada natural* $n \in \mathbb{N}$ *el cardinal del conjunto*

$$\{m \in \mathbb{N} : 1 \leq m < n, mcd(n, m) = 1\}$$

**Proposición 2.** *Sean* $p \in \mathbb{P}$ *y* $a, b, n \in \mathbb{N}$ *con* $mcd(a, b) = 1$. *Entonces:*

1. $\varphi(p) = p - 1$
2. $\varphi(p^n) = p^{n-1}(p - 1)$
3. $\varphi(ab) = \varphi(a)\varphi(b)$

**Teorema 3.** *Sean* $a, n \in \mathbb{N}$ *tales que* $mcd(a, n) = 1$. *Entonces* $n \mid a^{\varphi(n)} - 1$.

## Resultados de teoría de grupos

**Teorema 4.** *(Teorema de Lagrange) Sea* $G$ *un grupo y sea* $H < G$ *un subgrupo suyo. Entonces:*

- $G$ *es finito* $\Leftrightarrow$ $H$ *y* $[G : H]$ *son finitos.*
- $G$ *es finito* $\Rightarrow o(G) = o(H)[G : H]$.

**Teorema 5.** *(Teorema de Cauchy) Sea* $G$ *un grupo finito y sea* $p \in \mathbb{P}$ *tal que* $p \mid o(G)$. *Entonces* $\exists g \in G : o(g) = p$.

**Teorema 6.** *(Ecuación de clases) Sea* $G$ *un grupo finito y* $\rho : G \times G \to G : (g, h) \mapsto hgh^{-1}$ *una acción de* $G$ *sobre* $G$. *Sea* $G_0$ *el conjunto de los elementos de* $G$ *cuya órbita por* $\rho$ *sólo tiene un elemento, es decir, el centro de* $G$, $Z(G)$, *y sean* $\Theta_1, ..., \Theta_n$ *las órbitas con más de un elemento. Si tomamos un* $x_i$ *en cada* $\Theta_i$ *y denominamos* $I(x_i) = \{g \in G : gx_ig^{-1} = x_i\}$ *entonces*

$$o(G) = o(Z(G)) + \sum_{i=1}^{n} [G : I(x_i)]$$

**Corolario 7.** *Si* $G$ *es un p-grupo de Sylow entonces* $Z(G) \neq \{1_G\}$.

**Teorema 8.** *(Primer teorema de Sylow) Sean $G$ un grupo finito y un primo $p \in \mathbb{P}$ tal que hay un $r \in \mathbb{N}$ de modo que $p^r \mid o(G), p^{r+1} \nmid o(G)$. Entonces $\forall i \in \{1, ..., r\}\, \exists H_i < G$ verificando:*

- $|H_i| = p^i, \forall i \in \{1, ..., r\}$.
- $H_1 \triangleleft H_2 \triangleleft ... \triangleleft H_r$.

**Teorema 9.** *(Segundo teorema de Sylow) Sean $G$ un grupo finito y $P, H < G$ dos $p$-subgrupos suyos. Entonces $P$ y $H$ son conjugados, es decir, $\exists g \in G : P = gHg^{-1}$.*

**Teorema 10.** *(Tercer teorema de Sylow) Sean $G$ un grupo finito, $p \in \mathbb{P} : p \mid o(G)$ y $n_p$ el número de $p$-subgrupos de Sylow de $G$. Entonces:*

- $n_p = [G : \mathrm{N}_G(P)], \forall P < G$ *$p$-subgrupo de Sylow.*
- $n_p \mid [G : P], \forall P < G$ *$p$-subgrupo de Sylow.*
- $n_p \equiv 1(p)$

**Teorema 11.** *(Teorema de estructura de los grupos abelianos finitos) Sea $G$ un grupo abeliano finito. Entonces existen unos únicos $m_1, ..., m_r \in \mathbb{N}$ tales que $o(G) = m_1 ... m_r$, $m_i \mid m_{i+1}, \forall i \in \{1, ..., r-1\}$ y*

$$G \cong C_{m_1} \times ... \times C_{m_r}$$

# Bibliografía


[1] Michael Aschbacher. The status of the clasification of the finite simple groups. *Notices of the American Mathematical Society*, 51(7):pp. 736–740, 2004. http://www.ams.org/notices/200407/fea-aschbacher.pdf.

[2] Hans Ulrich Besche Bettina Eick and Eamonn A. O'Brien. A millennium project: constructing small groups. *International Journal of Algebra and Computation*, 12(5):pp. 626–644, 2002. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.9.8357&rep=rep1&type=pdf.

[3] Emilio Bujalance, José Javier Etayo, and Ernesto Martínez. Cyclic and dihedral actions on Klein surfaces with 2 boundary components. 2019. Preprint.

[4] Julio Castellanos. Estructuras algebraicas. *Universidad Complutense de Madrid*, 2017. https://www.ucm.es/data/cont/docs/90-2017-09-13-NotasProfesorEA-2017.pdf.

[5] Keith Conrad. The Schur – Zassenhaus theorem. *University of Connecticut*. https://kconrad.math.uconn.edu/blurbs/grouptheory/schurzass.pdf.

[6] Daniel Gorenstein. *Finite groups*. Harper Row, New York, Estados Unidos de América, 1968.

[7] Daila Silva Seabra de Moura Fonseca. *Grupos e seus automorfismos*. Universidade Federal de Minas Gerais, Belo Horizonte, Brasil, 2008.

[8] Jasha Sommer-Simpson. Automorphism groups for semidirect products of cyclic groups. 2013. http://math.uchicago.edu/~may/REU2013/REUPapers/Sommer-Simpson.pdf.

[9] John Sullivan. Classification of finite abelian groups. *The International Society of the Arts, Mathematics, and Architecture*, 2003. http://torus.math.uiuc.edu/jms/m317/handouts/finabel.pdf.